

عنوان المشروع:

دور الامن السيبراني في حماية الأنظمة المعلوماتية

The role of cybersecurity in protecting information systems

إعداد الطالب

سلطان سليمان عجمي

٢٣٣٠٠٠٢٠٢

إشراف

د. الفیصل عبد الحمید

د. فايز جراد

العام الدراسي:

٢٠٢٤

المحتويات

المحتويات	٢
فهرس الجداول	٦
فهرس الرسوم التوضيحية	٧
شكر وتقدير	٨
الإهداء	٩
الملخص باللغة العربية	١٠
الفصل الأول	١٢
خلفية الدراسة وأهميتها	١٢
مقدمة:	١٣
مشكلة الدراسة	١٥
أهمية الدراسة	١٦
الأهمية العلمية:	١٦
الأهمية العملية:	١٧
أهداف الدراسة	١٧
فرضية الدراسة:	١٨
الدراسات السابقة	١٩
١- دراسة (مرزوق، ٢٠٢٤) "إنعكاسات الأمن السيبراني على أمن المعلومات في البنوك"	١٩
٢- دراسة (التونى، ٢٠٢٣) "أثر وعي العملاء بالقرصنة الالكترونية كأداة لتحقيق الأمن السيبراني"	١٩
٣- دراسة (الحيمودي، ٢٠٢٣) "الامن السيبراني وحماية الأنظمة المعلوماتية"	٢٠
٤- دراسة (جبر، ٢٠٢٣) "تهديدات الامن السيبراني للمصارف الالكترونية وآلية مواجهاتها"	٢١
٥- دراسة (المنيع، ٢٠٢٢) "تحقيق الامن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠"	٢٢
٦- دراسة (جدو، ٢٠٢٢) "تحديات الامن السيبراني لمواجهه الجريمة الالكترونية"	٢٢
7- دراسة (علي، ٢٠٢٢) " الامن السيبراني والنظافة الرقمية"	٢٣
8- دراسة (السميري، ٢٠٢٢) " واقع الامن السيبراني وتحدياته في السعودية"	٢٤
9- دراسة (صالح، ٢٠٢٠) "دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية"	٢٤

دراسة (المري، ٢٠٢٤) "الأمن السيبراني وحماية الأنظمة الإلكترونية	10-
دراسة تحليلية تأصيلية"	٢٥
حدود الدراسة:	٢٧
الحدود الزمنية:	٢٧
الحدود البشرية:	٢٧
متغيرات الدراسة:	٢٧
- المتغير المستقل:	٢٧
- المتغير التابع:	٢٧
منهجية الدراسة:	٢٧
أدوات الدراسة:	٢٧
الفصل الثاني	٢٨
الإطار النظري	٢٨
مفهوم الامن السيبراني	٢٩
لغويًا:	٢٩
اصطلاحًا:	٢٩
تعريف الأمن السيبراني:	٢٩
تعريف الهيئة الوطنية للأمن السيبراني:	٣٠
أهمية الأمن السيبراني:	٣١
خصائص الجريمة السيبرانية:	٣٢
أساليب الأمن السيبراني العالمي:	٣٣
أهم أدوات الأمن السيبراني للحماية من الهجمات الإلكترونية:	٣٣
ما هي برامج مكافحة الفيروسات:	٤٠
البنية التحتية الحساسة:	٤١
خطوات تحديد أهداف الامن السيبراني:	٤٢
مهام إدارة البحوث والمراقبة في الأمن السيبراني:	٤٣
نشر خدمات الأمن السيبراني:	٤٣
مسؤولية مقدمي خدمات الامن السيبراني	٤٤
ماهية مزودي خدمات الاتصالات الإلكترونية:	٤٦
التزامات مقدمي خدمات الانترنت:	٤٧
حماية الأنظمة الإلكترونية:	٤٨
الجريمة السيبرانية كتهديد للأمن السيبراني:	٤٩

الأفعال التي تشكل الجريمة السيبرانية:	٥٠
التدابير الأمنية أمن المعلومات:	٥٢
التدابير الأمنية لأمن المعلومات في المملكة (الضوابط الأساسية للأمن السيبراني):	٥٢
الضوابط الأساسية للأمن السيبراني في المملكة العربية السعودية:	٥٤
أهداف الضوابط الأساسية للأمن السيبراني في المملكة العربية السعودية:	٥٤
نطاق العمل:	٥٥
قابلية التطبيق:	٥٥
مفهوم أمن نظم المعلومات	٥٦
مفهوم أمن المعلومات:	٥٧
ولإدارة امن المعلومات مجموعة من المتغيرات الداخلية التي تعمل على نجاح برامج أمن نظم المعلومات وهذه المتغيرات هي:	٥٧
برامج أمن المعلومات:	٦٠
برنامج امن المعلومات (وزارة الموارد البشرية في المملكة):	٦٣
رؤية واهداف إدارة امن المعلومات:	٦٣
الفصل الثالث:	٦٦
الإطار العملي للدراسة:	٦٦
مقدمة:	٦٧
أولاً: ترميز إجابات برنامج التحليل الاحصائي (SPSS):	٦٧
ثانياً: نسبة تكرار الاسئلة الشخصية:	٧٠
ثالثاً: نسبة تكرار أسئلة المحور الأول:	٧٣
رابعاً: نسبة تكرار اسئلة المحور الثاني:	٨٢
خامساً: إجابات المحور الثالث:	٩١
سادساً: معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الأول عبر برنامج التحليل الاحصائي (SPSS):	١٠٣
سابعاً: معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الثاني عبر برنامج التحليل الاحصائي (SPSS):	١٠٤
ثامناً: معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الثالث عبر برنامج التحليل الاحصائي (SPSS):	١٠٦
تاسعاً: اختبار فرضية الدراسة:	١٠٧
الفصل الرابع:	١٠٩
النتائج والتوصيات:	١٠٩
مقدمة:	١٠٩

١٠٩	أولا النتائج.....
١١١	ثانياً التوصيات:.....
١١٣	الفصل الخامس.....
١١٣	المراجع والملحقات
١١٣	المراجع
١١٣	المراجع باللغة العربية:.....
١١٧	المراجع باللغة الانجليزية:.....
١١٧	المراجع الالكترونية:.....
١١٨	الاستبانة:.....
١١٩	٢- المحور الأول: السياسات والاجراءات
١٢٠	المحور الثاني: إجراءات امن المعلومات المتعلقة بالعاملين.....
١٢١	المحور الثالث: إجراءات امن المعلومات المتعلقة بالعتاد والبيانات.....
١٢٢	الملخص باللغة العربية

فهرس الجداول

٦٧	جدول ١ البيانات الشخصية (النوع)
٦٨	جدول ٢ البيانات الشخصية (العمر)
٦٨	جدول ٣ البيانات الشخصية (المستوى التعليمي)
٦٩	جدول ٤ ترميز إجابات برنامج التحليل الإحصائي (SPSS)
٧٠	جدول ٥ تكرار الأسئلة الشخصية (النوع)
٧١	جدول ٦ تكرار الأسئلة الشخصية (العمر)
٧٢	جدول ٧ تكرار الأسئلة الشخصية (المستوى التعليمي)
٧٣	جدول ٨ نسبة تكرار أسئلة المحور الأول السؤال الأول
٧٤	جدول ٩ نسبة تكرار أسئلة المحور الأول السؤال الثاني
٧٦	جدول ١٠ نسبة تكرار أسئلة المحور الأول السؤال الثالث
٧٧	جدول ١١ نسبة تكرار أسئلة المحور الأول السؤال الرابع
٧٨	جدول ١٢ نسبة تكرار أسئلة المحور الأول السؤال الخامس
٧٩	جدول ١٣ نسبة تكرار أسئلة المحور الأول السؤال السادس
٨١	جدول ١٤ نسبة تكرار أسئلة المحور الأول السؤال السابع
٨٢	جدول ١٥ نسبة تكرار أسئلة المحور الثاني السؤال الأول
٨٣	جدول ١٦ نسبة تكرار أسئلة المحور الثاني السؤال الثاني
٨٤	جدول ١٧ نسبة تكرار أسئلة المحور الثاني السؤال الثالث
٨٦	جدول ١٨ نسبة تكرار أسئلة المحور الثاني السؤال الرابع
٨٧	جدول ١٩ نسبة تكرار أسئلة المحور الثاني السؤال الخامس
٨٨	جدول ٢٠ نسبة تكرار أسئلة المحور الثاني السؤال السادس
٨٩	جدول ٢١ نسبة تكرار أسئلة المحور الثاني السؤال السابع
٩٠	جدول ٢٢ نسبة تكرار أسئلة المحور الثاني السؤال الثامن
١٠٨	جدول 41 معامل الارتباط بيرسون بين المتغير المستقل والتابع
١٠٨	جدول ٤٢ معامل الارتباط بيرسون بين المتغير المستقل والتابع

فهرس الرسوم التوضيحية

٦٢	رسم توضيحي مكونات برنامج أمن المعلومات ١
٧٠	رسم توضيحي ١ نسبة التكرار للأسئلة الشخصية (النوع)
٧١	رسم توضيحي ٢ تكرار الأسئلة الشخصية (العمر)
٧٢	رسم توضيحي ٣ تكرار الأسئلة الشخصية (المستوى التعليمي)
٧٣	رسم توضيحي ٤ نسبة تكرار أسئلة المحور الأول للسؤال الأول
٧٥	رسم توضيحي ٥ نسبة تكرار أسئلة المحور الأول السؤال الثاني
٧٦	رسم توضيحي ٦ نسبة تكرار أسئلة المحور الأول السؤال الثالث
٧٧	رسم توضيحي ٧ نسبة تكرار أسئلة المحور الأول السؤال الرابع
٧٨	رسم توضيحي ٨ نسبة تكرار أسئلة المحور الأول السؤال الخامس
٨٠	رسم توضيحي ٩ نسبة تكرار أسئلة المحور الأول السؤال السادس
٨١	رسم توضيحي ١٠ نسبة تكرار أسئلة المحور الأول السؤال السابع
٨٢	رسم توضيحي ١١ نسبة تكرار أسئلة المحور الثاني السؤال الأول
٨٤	رسم توضيحي ١٢ نسبة تكرار أسئلة المحور الثاني السؤال الثاني
٨٥	رسم توضيحي ١٣ نسبة تكرار أسئلة المحور الثاني السؤال الثالث
٨٦	رسم توضيحي ١٤ نسبة تكرار أسئلة المحور الثاني السؤال الرابع
٨٧	رسم توضيحي ١٥ نسبة تكرار أسئلة المحور الثاني السؤال الخامس
٨٨	رسم توضيحي ١٦ نسبة تكرار أسئلة المحور الثاني السؤال السادس
٨٩	رسم توضيحي ١٧ نسبة تكرار أسئلة المحور الثاني السؤال السابع
٩١	رسم توضيحي ١٨ نسبة تكرار أسئلة المحور الثاني السؤال الثامن

شكر وتقدير

قال تعالى: ﴿وَإِذْ تَأَذَّنَ رَبُّكُمْ لَئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ وَلَئِنْ كَفَرْتُمْ إِنَّ عَذَابِي لَشَدِيدٌ﴾

الحمد لله القائل في كتابة " علم الانسان مالم يعلم وأصلى وأسلم على نبي الهدى والرحمة صلوات ربي وسلامه عليه، القائل في سنته، من سلك طريقاً يلتمس به علماً سهل الله له طريقاً إلى الجنة" صدق رسول الله

الشكر أولاً وأخيراً لله تعالى على فضله ونعمه التي لا تحصى، والحمد لله أن جعلنا مسلمين

اتقدم بالشكر الجزيل والعرفان الجميل إلى مشرف الدراسة والذي تفضل مشكور بالإشراف على هذه الدراسة التي كان لتوجيهه القيم وعطائه المخلص الاسهام الكبير في عمل هذه الدراسة.

وكما نتقدم بجزيل الشكر والامتنان لوالدينا لحرصهم الدؤوب على نجاحنا واهتمامهم ببناء طوال فترة الدراسة ونتقدم بجزيل الشكر لكل ما ساندنا ودعمنا في مسيرتنا الدراسة، لكم مننا خالص الامتنان والتقدير

الإهداء

إلى من ربياني صغيراً...

إلى والدينا والذين بذلوا الكثير في سبيل تربيتنا
وتعليمنا، وكانوا لنا المثل الذي غرسوا في نفسينا
علو الهمة وحب الطموح.

إلى اللذين صدقوني معاملتهم وكل من أهدى لي
حكمه، أو اسدى لي نصيحة، أو لقنني كلمة.

إلى أصدقائنا وزملائنا، وإلى كافة اساتذتنا
ومعلمينا

إلى كل هؤلاء نهدي ثمرة جهدنا المتواضع

الملخص باللغة العربية

تهدف هذه الدراسة إلى التعرف على مفهوم الامن السيبراني واهميته واساليبه والتعرف على مفهوم الأنظمة الالكترونية وكيفية عملها ومفهوم نظم المعلومات والتعرف على واقع دور الامن السيبراني في حماية الأنظمة المعلوماتية والتعرف على أساليب التطوير في حماية الأنظمة المعلوماتية والثغرات في حماية الأنظمة المعلوماتية والتعرف على آراء العاملين في تطوير حماية الأنظمة المعلوماتية والتعرف على فاعلية دور الامن السيبراني في حماية الأنظمة المعلوماتية والتعرف على أخطاء العاملين في حماية الأنظمة المعلوماتية، والتعرف على إيجابيات العاملين في حماية الأنظمة المعلوماتية، وتم الاعتماد في هذه الدراسة على المنهج الوصفي التحليلي عبر توزيع الاستبانة الكترونيا عبر جوجل فورمز وتحليلها في برنامج التحليل الاحصائي (SPSS) واستهدفت الاستبانة عينة عشوائية من الموظفين العاملين في مجال الحماية الالكترونية والبالغ عددهم (٥٠) عينة وقد توصلت الدراسة إلى جملة من النتائج كانت أهمها: أن الإدارة الجيدة في استخدام التكنولوجيا يساهم بدرجة كبيرة في رفع دور الامن السيبراني في حماية الأنظمة المعلوماتية وتبين أنه هناك رقابة مباشر من المدراء على عمل الموظفين مما ينعكس إيجابا في دور الامن السيبراني في حماية الأنظمة المعلوماتية وأن الدورات التدريبية للموظفين تساهم بشكل كبير في حماية نظم المعلومات، وان مواكبة التطورات والبرامج الحديثة يساهم في الحد من المخاطر على نظم المعلومات.

الكلمات المفتاحية:

الأمن السيبراني، الأنظمة المعلوماتية.

Abstract:

This study aims to identify the concept of cybersecurity, its importance and methods, and to identify the concept of electronic systems and how they work, the concept of information systems, and to identify the reality of the role of cybersecurity in protecting information systems, and to identify the methods of development in protecting information systems and the gaps in protecting information systems, and to identify the opinions of workers in developing the protection of information systems, and to identify the effectiveness of the role of cybersecurity in protecting information systems, and to identify the mistakes of workers in protecting information systems, and to identify the positives of workers in protecting information systems. This study relied on the descriptive analytical approach by distributing the questionnaire electronically via Google Forms and analyzing it in the statistical analysis program (SPSS). The questionnaire targeted a random sample of employees working in the field of electronic protection, numbering (50) samples. The study reached a number of results, the most important of which were: that good management in the use of technology contributes greatly to raising the role of cybersecurity in protecting information systems, and it was found that there is direct supervision by managers over the work of employees, which is positively reflected in the role of cybersecurity in protecting information systems, and that training courses for employees contribute greatly to protecting information systems, and that Keeping up with developments and modern programs contributes to reducing risks to information systems.

الفصل الأول

خلفية الدراسة وأهميتها

مقدمة:

يشهد مستخدمي الأنظمة المعلوماتية في العصر الحديث تحولات سريعة نحو استخدام الامن السيبراني حيث تعتبر قضية أمن وحماية الأنظمة المعلوماتية من أهم واصعب القضايا التي تواجه مستخدمي الأنظمة المعلوماتية، حيث يقاس نجاح المؤسسات أو البنوك أو الشركات على ما تمتلكه تلك الشركات أو المؤسسات أو البنوك من معلومات، لاكن من التحديات التي يواجهها مستخدمي الأنظمة المعلوماتية انها أكثر عرضة للخطر بين الحين والآخر، حيث تواجه الكثير من الخروقات لتلك الأنظمة مثل (الهكرز) أو غيرها من المنظمات حيث تعمل على تعطيل تلك الأنظمة وتدمير قاعدة بياناتها خلال ثواني معدودة، حيث تختلف تلك الهجمات من مكان لآخر ومن وقت إلى وقت، وتحدث تلك الهجمات مع تسارع الوقت والزمن، وهنا يأتي الدور الهام للأمن السيبراني للحفاظ على مستخدمي الأنظمة المعلومات وعمل حاجز وسد منيع لتلك الهجمات وسلامة مستخدمي الأنظمة المعلوماتية وحقوق المواطنين.

وفي هذا الاطار استهدفت رؤية المملكة العربية السعودية ٢٠٣٠ التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه وعيشهم الكريم، حيث ادركت المملكة بقيادتها العظيمة ومكانة المملكة الإقليمية والدولية ونمو قوتها الاقتصادية قد جعلتها مستهدفة للإضرار بأمنها واقتصادها وتنميتها ومن ذلك الاستهداف السيبراني الذي يتزايد عالميا، وهو ما جعل الامن السيبراني أولوية لكافة الدول بهدف تعزيز فضائها السيبراني وحمايته من المخاطر والتهديدات المتنوعة والابعاد الجيوسياسية، ولقد اصحب التهديدات والهجمات السيبرانية أكثر تطورا وخطرا على دول العالم وانظمتها ومؤسساته، وعبر طرق مبتكرة لم تعهد من قبل ويتوقع تزايد ذلك مستقبلا.

إذ تتشارك هذه الجهات والكيانات الآليات والتقنيات بشكل سريع حول العالم لشن هجماتها، وحيث ادركت المملكة بقيادتها الرشيدة والحكمة ذلك، وأدركت أن الامن السيبراني أضحي هدفا ومقوما أساسيا لتعزيز هذه المكانة ولحماية المصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة

والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية، فقد قامت بتعزيز الجهود والأنشطة في مجال الأمن السيبراني خلال الفترة الماضية، وكان من أبرز هذه الجهود إنشاء الهيئة الوطنية للأمن السيبراني واعتماد تنظيمها وجعلها مرتبطة بالملك أيده الله - بحيث تكون الجهة المختصة بالأمن السيبراني، والمرجع الوطني في شؤونه (السيبراني، ٢٠٢٠).

ولأجل حل هذه الإشكالية التي طرأت في عالمنا الحديث والتي تم التركيز عليها من معظم الدول هي التركيز على دراسة الأمن السيبراني وتعتبر من أحد الدراسات الحديثة التي طرأت في القرن الواحد والعشرين، فقد شهدت تطوراً كبيراً ومستمرًا ولا يمكن أن نغفل عنه، ولا بد في هذا المقام أن نشير إلى وجود جانب آخر مظلّم لذلك التطور الرقمي الذي يشهده العالم، ذلك الجانب يمكن أن يجعل الكثير من الدول الكبرى والشركات الناجحة والمؤسسات التجارية والاقتصادية مهددة بالاختراق، ولعل ذلك من أسباب أهمية دراسة الأمن السيبراني، والذي من أهم وظائفه الأساسية أن يعمل على حماية البيانات والشبكات والأنظمة الإلكترونية المختلفة من الهجمات والاختراقات التي قد تؤدي بها وباستقرارها (المنيع، ٢٠٢٢).

علاوة على ذلك، سلطت هذه الدراسة الضوء على توفير أهم المتطلبات لتحقيق رؤية ٢٠٣٠ في إبراز الأمن السيبراني وتحقيقه، وتطوير البنية التحتية للأمن السيبراني والحد من التجسس والاختراق والقرصنة مستقبلاً من خلال تطوير البرامج والتطبيقات بشكل مستمر والتعرف على أحدث التقنيات في مواجهة تلك القرصنات التي من الممكن حدوثها مستقبلاً.

بالإضافة إلى ذلك، تمحورت الدراسة حول تحليل البيانات المتلقاة من العينة المختارة من الموظفين في محل الدراسة، وذلك في تحليل ودراسة أفكارهم وأدوارهم فيما يتعلق بحماية الأنظمة المعلوماتية. من خلال هذه التحليلات، قدمت الدراسة إضاءة مفصلة على دور الأمن السيبراني في حماية الأنظمة المعلوماتية، وقدمت توصيات عملية ولموسة للمؤسسات العاملة بنفس المجال. ويهدف ذلك إلى تعزيز دور الأمن السيبراني في حماية الأنظمة المعلوماتية.

مشكلة الدراسة

على الرغم من التقدم الكبير في مجال الامن السيبراني، يظل هناك تحديات تواجه مستخدمي الأنظمة المعلوماتية. يتساءل البحث حول دور الامن السيبراني في حماية الأنظمة المعلوماتية والحد من المخاطر الأمنية التي تحدث بها.

أدى تطور التقنية وانتشارها في المؤسسات، دون وجود أنظمة حماية بتلك المؤسسات أو الشركات إلى تعرضها للكثير من المخاطر والتهديدات الأمنية وكذلك الاختراقات، مما فرض على تلك المؤسسات تحديات تتمثل في ضرورة الحفاظ على معلوماتها وبياناتها المخزنة على تلك الأجهزة مع التحديث المستمر لأنظمتها حتى لا تكون عرضة للتهديدات والمخاطر وكذلك الفيروسات، وتتعرض تلك المؤسسات لمخاطر الاختراقات والتي قد تكون ناتجة عن الادخال المتكرر للبيانات الخاطئة، الدخول لمواقع محجوبة، الفيروسات، التدريب غير الكاف للعاملين على هذه الشبكات ونقص الوعي التقني، مما يؤدي إلى تسلل قرصنة الأنظمة والمواقع لتلك المؤسسات مع تعرض بياناتها للتلف والتخريب نتيجة لتلك الاختراقات والتهديدات الأمنية لأنظمتها الالكترونية (المنيع، ٢٠٢٢).

وفي ظل التحولات السريعة التي تشهدها الشركات نحو استخدام الامن السيبراني وتكنولوجيا المعلومات، فقد أصبحت هذه القضية من أصعب القضايا التي تواجهها تلك الشركات أو المؤسسات العاملة في مجال الأنظمة المعلوماتية فتعتبر مشكلات أمن المعلومات انها تحتوي على الكثير من الأمور التقنية والبشرية والتنظيمية، ويمكن ان يكمن الحل عبر تحسين أفضل لإدارة نظم المعلومات ويمكن تحسينها في تقييم وإدارة تلك المخاطر التي يمكن ان تواجهها والعمل على إيجاد الحلول الأمنية والمعلوماتية، ومراجعة أنظمة الرقابة والتحكم.

ويمكن صياغة مشكلة الدراسة على عدة أسئلة نصيغها على التساؤلات
الآتية:

- ماهية الأمن السيبراني؟
- ماهية الأنظمة المعلوماتية؟
- ما هو دور الامن السيبراني في حماية الأنظمة المعلوماتية؟
- ماهي طرق تطوير دور الامن السيبراني في حماية الأنظمة
المعلوماتية؟

أهمية الدراسة

من خلال طبيعة الدراسة وأهميتها يمكننا ان نقسم أهمية الدراسة إلى
قسمين:

الأهمية العلمية:

تكمّن الأهمية العلمية في ان هذه الدراسة تعد من المواضيع المهمة والجديدة
على الساحة البحثية ويعمل على تقديم إطار نظري لدور الامن السيبراني
في حماية الأنظمة المعلوماتية، وما يمكن ان تضيفه للتحسين في حماية
الأنظمة المعلوماتية في المملكة ودراسة العديد من الدراسة السابقة المتعلقة
بنفس الموضوع ومدى تأثيرها في حماية الأنظمة المعلوماتية، والتي ستعمل
أيضا على الاهتمام بتحسين حماية الأنظمة المعلوماتية من الهجمات
السيبرانية.

الأهمية العملية:

- توضيح أهمية دور الامن السيبراني في حماية الأنظمة المعلوماتية.
 - التوصل إلى نتائج وتوصيات يمكن أن تفيد المسؤولين في.
 - مساعدة المشرفين والقائمين على التعرف على واقع الامن السيبراني.
 - معرفة وجهة نظر العاملين وآرائهم في تطوير دور الامن السيبراني في حماية الأنظمة المعلوماتية والاستفادة منها وايصالها للقائمين في الجامعة.
- وتمثل أيضا في تبين نقاط القوة المتمثلة في دراسة الحالة (الاستبانة) عن التطبيق في الواقع العملي ودور الامن السيبراني في حماية الأنظمة المعلوماتية.

أهداف الدراسة

تهدف الدراسة إلى تحقيق عدة أهداف أهمها:

- التعرف على واقع دور الامن السيبراني في حماية الأنظمة المعلوماتية.
- التعرف على أساليب التطوير في حماية الأنظمة المعلوماتية.
- التعرف على مفهوم الأمن السيبراني وأهمية الامن السيبراني وأساليب الأمن السيبراني.
- التعرف على ماهية الأنظمة الالكترونية وكيفية عملها، ومفهوم نظم المعلومات.
- التعرف على الثغرات في حماية الأنظمة المعلوماتية.
- التعرف على آراء العاملين في تطوير حماية الأنظمة المعلوماتية.

- التعرف على فاعلية دور الامن السيبراني في حماية الأنظمة المعلوماتية.

- التعرف على أخطاء العاملين في حماية الأنظمة المعلوماتية.

- التعرف على إيجابيات العاملين في حماية الأنظمة المعلوماتية.

فرضية الدراسة:

- هناك علاقة ارتباطية موجبة بين استخدام الامن السيبراني ودوره في حماية الأنظمة المعلوماتية.

الدراسات السابقة

١- دراسة (مرزوق، ٢٠٢٤) "انعكاسات الأمن السيبراني على أمن المعلومات في البنوك"

تهدف هذه الدراسة إلى تبيان تأثير الأمن السيبراني على أمن المعلومات في البنوك، حيث تم اختيار المجمع الجهوي لبنك بدر - تبسة - لإجراء الدراسة التطبيقية، في حين تم استخدام الاستبيان كأداة لجمع البيانات، وتم توزيع الاستبيان على موظفي المؤسسة بواقع ٥٠ استمارة، وقد تم استخدام المنهج الوصفي التحليلي وأيضا المنهج الاحصائي للوصول إلى نتائج واختبار الفرضيات وذلك من خلال الاستعانة بالبرنامج الاحصائي (SPSS).

وحصلت الدراسة إلى نتائج كانت أهمها:

- وجود علاقة ذات دلالة إحصائية بين الامن السيبراني وأمن المعلومات في البنوك.
- يساهم الامن السيبراني في حماية المعلومات البنكية من الهجمات السيبرانية.

٢- دراسة (التوني، ٢٠٢٣) "أثر وعي العملاء بالقرصنة الالكترونية كأداة لتحقيق الأمن السيبراني"

إن القرصنة الالكترونية أصبحت من أهم التحديات التي تؤرق الدول والمجتمعات وبصفة خاصة المهتمين بتكنولوجيا المعلومات، لأنها تمس المعلومات التي باتت تمثل أهم العناصر الاستراتيجية في عصر المعلوماتية، هدف البحث إلى التعرف على أثر وعي العملاء بالقرصنة الالكترونية كأداة لتحقيق الامن السيبراني في البنوك الحكومية بمحافظة بوردعيد مع اختبار العلاقة ميدانيا بين المتغيرين ومعرفة مدى العلاقة بين ابعاد وعي العملاء بالقرصنة الالكترونية، وتكون مجتمع البحث من العملاء بالبنوك الحكومية بمحافظة

بورسعيد، وتم توزيع (٤٥٠) واستخدام برنامج التحليل الاحصائي (SPSS) للإجابة على أسئلة البحث، وخلصت لمجموعة من النتائج كان ابرزها بأن مستوى ودور إدارة الحماية البنكية كان مرتفعاً، وكذلك بينت البحث وجود دور الامن السيبراني بدلالة ابعاده في التوعية والحد من الجرائم المالية، أظهرت نتائج تحليل الاحصائي بأن فاعلية إجراء الرقابة الداخلية في توفير الأمن السيبراني في التصدي للجرائم (القرصنة الالكترونية) وذلك من خلال توفير آليات مناسبة لتطوير معارف ومهارات للعملاء الحاليين والمستقبليين ورفع مستوى الوعي والإرشاد وتمكينهم من فهم المخاطر الأساسية للمعاملات التي يجرونها مع البنوك والتصدي من عمليات الاحتيال التي يعرض لها العملاء وكيفية توفير وتوضيح الطرق التي من خلالها يقوم المحتالون بخداع ضحاياهم، وبما يمكن العملاء من التصيد لعملية الاحتيالي وقدرتهم على اتخاذ القرارات المناسبة لهم، وتوجيههم إلى الجهة المناسبة للحصول على المعلومات في حال حاجتهم ولذلك وبناء على نتائج البحث فقد تمت صياغة عدد من التوصيات من أهمها: ضرورة تضافر الجهود بين القطاعات الحكومية ومن ضمنها البنوك في التعاون والتنسيق فيما بينها لأجل تطوير وتحسين إدارة الامن السيبراني والقدرة على توفير الثقافة البنكية ودورها في تحقيق التوعية المصرفية والتصدي للقرصنة الالكترونية بالإضافة إلى زيادة الأبحاث المرتبطة بالأمن السيبراني إذ تبين قلة في هذه الدراسات وخصوصا العربية منها.

٣- دراسة (الحيمودي، ٢٠٢٣) "الامن السيبراني وحماية الأنظمة المعلوماتية"

ان التقدم الكبير في تكنولوجيا المعلومات والاتصالات جعل من الامن السيبراني أهمية كبيرة للمجتمع المغربي وللمملكة المغربية، حيث ان الامن السيبراني مهم على مستوى الفرد في حماية البيانات الشخصية والصور والملفات والفيديوهات والحسابات الشخصية وكلمات المرور والحسابات البنكية وغيرها من الامور التي ترتبط بحياة المواطن

المغربي، وعلى مستوى المجتمع المغربي، من حيث حماية المجتمع من الهندسة الاجتماعية واستهداف السلوك الاجتماعي والبيانات المجمعة والخصوصيات للمجتمع، وعلى مستوى الشركات والمؤسسات، في حماية الأصول الإلكترونية والبيانات والمعلومات وبيانات الموظفين والعملاء والمواقع الإلكترونية، وعلى مستوى الدولة، في حماية أمنها الإلكتروني وحماية الأنظمة المالية والاقتصادية وغيرها من الهجمات الإلكترونية والابتزاز والقرصنة والتعطيل، وبما أن الأمن السيبراني عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير فإننا سنتعرف في هذا البحث على مدى تكريس الأمن السيبراني على المستوى الوطني والدولي وذلك لمعرفة مدى ملاءمة المشرع المغربي للاتفاقيات والمعاهدة الدولية.

٤- دراسة (جبر، ٢٠٢٣) "تهديدات الامن السيبراني للمصارف الإلكترونية وآلية مواجهاتها"

يهدف هذا البحث إلى عرض أهم التحديات التي تواجه المجتمع المصرفي من أجل تحقيق الامن السيبراني والذي يلعب دوراً محورياً في معالجة التحديات المستقبلية نظراً لاستخدامه كتكنولوجيا لإدارة الشبكات، وذلك لمحاولة وضع آليات للحد من هذه المخاطر، واتخاذ كافة الإجراءات الاحترازية التي يمكن ان تزعزع سلامة ونزاهة واستقرار القطاع المصرفي والمالي، حيث تمثل التكنولوجيا المالية وتطبيقاتها المالية المختلفة فرصاً وتحديات في الوقت الراهن، وذلك بما يدعم أهداف التنمية المستدامة في ظل رؤية ٢٠٣٠.

٥- دراسة (المنيع، ٢٠٢٢) "تحقيق الامن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠"

تتمثل أهمية الدراسة الحالية في التعرف على واقع تحقيق الامن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠ وقد قامت الباحثة باتباع المنهجية الوصفية التحليلية، وتكون المجتمع البحثي للدراسة من جميع الموظفين التقنيين لثلاث جامعات سعوديات، هي (جامعة ام القرى، جامعة الامام عبدالرحمن بن فيصل، جامعة الامام محمد بن مسعود الإسلامية)، وقد بلغ عددهم (٤٦٨) موظفاً، واعتمدت الدراسة أسلوب العينة العشوائية، وقد بلغ عدد العينة (٢١٠) موظفين، كما اعتمدت الاستبانة أداة للدراسة، ومن خلال نتائج الدراسة، توصلت إلى أن مفردات العينة موافقون بدرجة متوسطة على واقع تحقيق الامن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠ وتبين ان مفردات العينة موافقة بدرجة كبيرة جداً على معوقات تحقيق الامن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠ من أهم هذه المعوقات تدني مستوى الخبرة لدى الموظفين، والضعف في التعاون بين موظفي التقنيات في الجامعات لتحقيق الامن السيبراني، كما بينت النتائج وجود اتفاق بدرجة كبيرة جداً بين مفردات عينة الدراسة على متطلبات تحقيق الامن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠، وقدمت الدراسة مجموعة من المقترحات، كان من أهمها توعية العاملين بمخاطر استخدام الأجهزة الشخصية، المتمثلة في الهاتف المحمول لنقل او تخزين معلومات سرية خاصة بالجامعة، ومنح الحوافز المادية والمعنوية المناسبة التي تعمل على دعم وتشجيع الموظفين المتميزين والمبدعين في مجال الامن السيبراني.

٦- دراسة (جدو، ٢٠٢٢) "تحديات الامن السيبراني لمواجهة الجريمة الالكترونية"

تهدف هذه الدراسة إلى استكشاف واقع وتحديات الامن السيبراني على المستوى الدولي والمحلي، خاصة مع التطور التكنولوجي

واندماجه في مختلف المجالات السياسية، الاقتصادية والاجتماعية، فتوفير الحماية لمستخدمي التكنولوجيا في الوقت المعاصر أصبح ضرورة يجب أخذها بعين الاعتبار، في ظل توسع استخدام شبكة الانترنت وتنامي ما يعرف بالجريمة الالكترونية والإرهاب السيبراني.

خلصت هذه الدراسة إلى أن هناك جهود دولية للحد من آثار الجريمة الالكترونية على المستوى الدولي من خلال مجموعة من الهيئات والمنظمات الدولية مثل جهود الأمم المتحدة، الاتحاد الأوروبي، من خلال مجموعة من الاتفاقيات والتوصيات الدولية، وكذا على المستوى المحلي من خلال سن قوانين في هذا السياق، وأنشاء هيكل مختصة في محاربة الجريمة الالكترونية في الجزائر.

٧- دراسة (علي، ٢٠٢٢) " الامن السيبراني والنظافة الرقمية"

تتناول الدراسة موضوع الامن السيبراني والنظافة الرقمية نظراً لأهميته الكبير في ظل التحديات الراهنة التي تواجه المستخدمين نتيجة تعاملاتهم مع شبكات الانترنت والأجهزة حيث تزداد عمليات الاختراق والانتهاكات يوماً بعد يوم ومن ثم كان لازماً أن يكون هناك درعاً لها وهنا يأتي دور الامن السيبراني والنظافة الرقمية، ومن ثم هدفت هذه الدراسة إلى التعرف على مفهوم كلاً من الامن السيبراني والنظافة الرقمية ومعرفة الفرق بينهما، الوقوف على أهم الهجمات التي تعترض عملية الامن السيبراني وكذا المشكلات التي تواجه النظافة الرقمية، وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، وخرجت بعدة نتائج أهمها أن النظافة الرقمية جزء من الامن السيبراني، أنه يوجد علاقة فيما بين النظافة الرقمية والامن السيبراني والذكاء الاصطناعي، وقد أوصت الدراسة بضرورة تكثيف دورات التوعية بموضوع الامن السيبراني والنظافة الرقمية للحد من الانتهاكات.

٨- دراسة (السميري، ٢٠٢٢) " واقع الامن السيبراني وتحدياته في السعودية "

يشهد العالم اليوم تسارعا المتزايد للأجهزة والمنصات والتطبيقات الإلكترونية، إذ أصبحت هذه التقنيات من العناصر المهمة في التحول الرقمي للعديد من الجهات الحكومية. لذلك صاحب هذه التطورات التقنية تطورات مماثلة في تقنيات الجرائم السيبرانية، تلك التي أضحت قضية دولية تحظى بالمزيد من الاهتمام وإحدى أولويات الأمن الوطني على صعيد العديد من دول العالم. ولأهمية هذه القضية، صدر أمر سامي كريم بإنشاء إدارة للأمن السيبراني في الجهات الحكومية في المملكة العربية السعودية وهدفها الرئيس حماية الأصول المعلوماتية والتقنية، ذلك ما يجعل الأمن السيبراني أحد أهم العناصر في تحقيق رؤية المملكة ٢٠٣٠. تأتي هذه الدراسة لتسليط الضوء على واقع الأمن السيبراني وتحدياته في المملكة، ولتحقيق أهداف هذه الدراسة تم تصميم استبانة إلكترونية تشمل المحاور الرئيسة التالية: إدارة الأمن السيبراني، تعامل إدارة الأمن السيبراني مع التهديدات والمخاطر السيبرانية، التقنيات أو الأساليب الأمنية المتبعة لإدارة التهديدات والمخاطرة السيبرانية، والتحديات المستقبلية (الاستراتيجية) لإدارة الأمن السيبراني. وبعد التحقق من صدق الاستبانة وثباتها، تم إلى عينة الدراسة، وقد شارك في الاستبانة بعدد (٩٨) إرسالها إلكترونياً من موظفي تقنية المعلومات ممن يعملون في جهات حكومية مختلفة. وقد أظهرت نتائج التحاليل الإحصائية أن مستوى واقع الأمن السيبراني في المملكة مرتفع لمواجهة التهديدات والمخاطر السيبرانية.

٩- دراسة (صالح، ٢٠٢٠) "دراسة أثر إدارة أمن المعلومات على نجاح برنامج نظم المعلومات المحاسبية"

يهدف البحث إلى محاولة معرفة أثر إدارة أمن المعلومات على نجاح برنامج أمن المعلومات في بيئة الأعمال المصرية، ولقد قدم البحث إطاراً نظرياً لأهم العوامل والمتغيرات التي تؤثر على فعالية إدارة أمن المعلومات، كما قام البحث باختبار عناصر ذلك الإطار ميدانياً على عينة

من فروع الشركة المصرية للاتصالات، وذلك باستخدام قائمة الاستقصاء التي تم تصميمها خصيصاً لهذا الغرض، ولقد تم تجميع البيانات اللازمة لاختبار الفروض الإحصائية باستخدام برنامج التحليل الإحصائي (SPSS) وعمل التحليل الإحصائي الوصفي وكذلك الاختبارات الإحصائية العلمية لاختبار الفروض، وقد توصلت نتائج الدراسة إلى أن إدارة أمن المعلومات لها تأثير جوهري وإيجابي على نجاح برنامج أمن نظم المعلومات المحاسبية في البيئة المصرية، كما أوصت بضرورة اهتمام منظمات الأعمال بإدارة أمن المعلومات باعتبارها عنصراً هاماً وضرورياً لنجاح برنامج أمن المعلومات في منظمات الأعمال المصرية.

١٠- دراسة (المري، ٢٠٢٤) "الأمن السيبراني وحماية الأنظمة الإلكترونية دراسة تحليلية تأصيلية"

الأمن في الفضاء السيبراني أمر اهتمت به الدول في كل مكان في العالم، بغض النظر عن مدى تواجدهم في هذا الفضاء، مما يعنى ارتباط أمن المعلومات ارتباطاً عضوياً بالأمن القومي في معظم دول العالم، ذلك أن الاعتداء على البنى التحتية المهمة منها الاتصالات الأنظمة الإلكترونية يمكن أن يؤثر على كل الدول في منطقة جغرافية معينة، المؤثر بدوره المباشر على مصالح الدولة المعنية بالفضاء السيبراني، والتي تشكل بنيتها التحتية للاتصالات والمعلومات جزءاً من تركيبة البنية التحتية للفضاء السيبراني.

لذا احتل الاهتمام بأمن المعلومات المراكز الأولى في اهتمامات واضعي السياسات العامة في أغلب الدول، وعلى كل المستويات سواء الإقليمية أو المحلية، فالدولة لأنها المنتج الأكبر للبيانات والمعلومات العامة والخاصة، هي المعنية بالأمن السيبراني، كما أنها المتحكمة في وضع النظم والقواعد التي تحدد الضوابط والحدود.

ومما لا شك فيه أن العالم أصبح يعاني من مشكلات اجتماعية أفرزتها البيئة الرقمية، بيد أن هذه المشكلات أصبحت مساراً للبحث والدراسة

لاسيما في مجال علم الاجتماع، ففي ظل ما يشهده العالم من تطور سريع ومتزايداً في النظم الذكية والأجهزة الإلكترونية وما صاحبهما من هجمات وجرائم سيبرانية مثل الغزو الثقافي الرقمي، والجريمة السيبرانية والابتزاز والتنمر عبر الأنظمة الإلكترونية، غدت الضرورة ملحة لنشر دعائم الأمن السيبراني وتأمين سلامة الممارسة الإلكترونية، وفي ضوء هذه البيئة المتغيرة ثمة حاجة ملحة لاتخاذ إجراءات على الصعيدين المحلي والدولي لحماية الاستهلاك والخصوصية ومجابهة تقنية المعلومات ضد جميع أشكال الجريمة السيبرانية.

حدود الدراسة:

الحدود الزمنية: تم عمل هذه الدراسة في العام ٢٠٢٤م.

الحدود البشرية: بعض العاملين في مجالات الامن السيبراني.

متغيرات الدراسة:

تتمثل متغيرات الدراسة في متغيرين:

- المتغير المستقل: الامن السيبراني.

- المتغير التابع: حماية الأنظمة المعلوماتية.

منهجية الدراسة:

تمثلت منهجية الدراسة في الاعتماد على المنهج الوصفي التحليلي، حيث تمت معالجة البيانات التي تم جمعها من خلال الاستبانة التي تم توزيعها عبر استخدام برنامج التحليل الاحصائي (SPSS) حيث بلغت عينة الدراسة (٥٠) عينة.

أدوات الدراسة:

اعتمدت الدراسة في جمع البيانات على الاستبانة التي تم تصميمها خصيصاً لاختبار فرضية الدراسة، والتي تم إعدادها بناء على مراجعة الدراسات السابقة والأبحاث والتقارير والمجلات العلمية المتخصصة في الموضوع. وتم تجميع البيانات عن طريق توزيع الاستبانة عبر (Forms Google) وقياس آراء المبحوثين عن طريق الاستبانة التي تم إعدادها وتم توزيعها على عينة عشوائية من بعض العاملين في نفس المجال.

الفصل الثاني

الإطار النظري

مفهوم الامن السيبراني

لغويًا:

مكون من لفظين يعنيان الأمن، وهو النقيض لكلمة الخوف، والأمن مصدر الفعل أمن أمنًا وأماناً وأمنة: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر، أي سلم منه.

اصطلاحاً:

تعددت التعاريف التي تناولت مصطلح السيبرانية كل حسب الزاوية التي نظر إليها منها، إلا أنها اشتركت في مضمون واحد متقارب في المعنى وهو استهداف مواقع الكترونية من خلال وسائل إلكترونية أخرى، وهي مجموعة من الممارسات التي ترمى إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية أيّاً كان نوعها وهذه الممارسات متنوعة إلى تدابير احتياطية استباقية قبل وقوع الخلل، وعلاجه بعد وقوع الخلل (المري، ٢٠٢٤).

تعريف الأمن السيبراني:

يُعرف بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنية الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والاضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج ولا تتحول الإضرار إلى خسائر دائمة، بالإضافة إلى ما ذكر في التقرير الصادر عن الاتحاد الدولي للاتصالات حول "اتجاهات الإصلاح في الاتصالات للعام ٢٠١٠-٢٠١١، حيث أنه يُعد مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات فضلى وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين (السيبراني، ٢٠٢٤).

تعريف آخر:

هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من

بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك (الرقمية، ٢٠٢٤).

تعريف الهيئة الوطنية للأمن السيبراني:

يعتبر مصطلح الأمن السيبراني مفهوم حديث دخل في بداية القرن العشرين حيث بدأ ظهوره بالثورة التكنولوجية، وقد اختلفت التعريفات لهذا المصطلح باختلاف طبيعة الدول ونورد بعضاً من هذه التعريفات كما يلي:

١. تعريف ليثيو مارتتي Martti Letho ونييتانماكي بيكا Neittaanmaki Pekka:

حيث تم تعريفه بأنه " مجموعة من الاجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة (ضرورسو، ٢٠٢٢)"

٢. تعريف ادوارد امورسو:

حيث تم تعريفه بأنه "هو الوسيلة التي من شأنها الحد من خطر الهجوم على اجهزة الحاسوب او الشبكات ويشمل في ذلك الادوات والوسائل المستخدمة في مواجهة القرصنة (ضرورسو، ٢٠٢٢)"

٣. تعريف الوكالة الفرنسية لأمن الاعلام:

بأنه فضاء التواصل المشكل من خلال الرابط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية (ضرورسو، ٢٠٢٢).

٤. تعريف وزارة الدفاع الامريكية:

جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها من مختلف الجرائم، الهجمات، التخريب، التجسس، الحوادث (مرزوق، ٢٠١٨).

٥. أما الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية:

عرف تنظيم الهيئة للأمن السيبراني على أنه "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوها (السيبراني، ٢٠٢٠).

أهمية الأمن السيبراني

يرتبط الأمن المعلوماتي بالجريمة الإلكترونية التي هي أساس الأمن المعلوماتي الذي يعمل على مكافحتها، وعي عبارة عن جرائم ذكية تنشأ في البيئة الإلكترونية أو الافتراضية، حيث قوم بها أفراد أو منظمات لديهم درجة عالية من الذكاء ويمتلكون المعرفة والتقنية، مما يتسبب في خسائر فادحة للمجتمع، وتظهر أهميته في عالمنا المترابط بواسطة الشبكة العنكبوتية، حيث أصبح يمثل عنصراً مهماً في الحياة الإنسانية على كافة المستويات السياسية والاقتصادية والاجتماعية، فهو الآن عصب الحياة الحالية التي تعتمد عليها الدول والأفراد في كل معاملاتها، بل بات ينظر إليه بأنه رافد جديد للأمن القومي، وجزء من الأمن الجماعي، بما أن العلاقة بين الأمن والتكنولوجيا علاقة مترابطة ومتزايدة، مع إمكانية تعرض المصالح الاستراتيجية إلى مخاطر إلكترونية، الأمر الذي يهدد بتحول دور الأنظمة الإلكترونية لوسيط ومصدر لأدوات الصراع الدولي، ودوره في تغذية التورات الدولية (فرحات، ٢٠٢١).

نظراً لكون المملكة العربية السعودية تتجه نحو التحول الرقمي في كثير من القطاعات، وتسعى المملكة لتكون ضمن مصاف دول العالم في الاقتصاد الرقمي من خلال الاستثمار في القطاعات التقنية، لذلك الهيئة تحمل على عاتقها حماية مصالح مستخدمي خدمات الاتصالات وتقنية المعلومات ولأن الاستدامة هي مسؤولية الجميع وجزء من ثقافة الهيئة، وتسعى الهيئة بشكل مستمر إلى تحقيق التأثير الإيجابي على المجتمع والمحافظة على استدامة البيئة وللضمان وسلامة المستخدمين من خلال إطلاق مبادرات تتماشى مع أفضل الممارسات العالمية في الأمن السيبراني (الرقمية، ٢٠٢٤).

خصائص الجريمة السيبرانية:

الجريمة السيبرانية هي امتداد طبيعي لنمو أجهزة الكمبيوتر، وقد نمت الجريمة السيبرانية بشكل هائل على مدى العقدين الماضيين، وتطورت الجريمة من قضية ثانوية إلى ظاهرة عالمية، مما يؤثر على أعداد غير مسبوقة من الأفراد وتسبب الملايين من حالات الأذى في كل عام، ومن آثار هذه الجرائم السيبرانية تتراوح الخسارة المالية بالمليارات وخسارة الكثير من الوقت في سرقة الهوية والاحتيال، وتسبب في الاضطراب العاطفي المرتبط بالقلق، والاكتئاب، أو حتى الأفكار الانتحارية مثل التحرش عبر الإنترنت أو العنف الإلكتروني والتعريض لوسائل الإعلام المتطرفة (المري، ٢٠٢٤).

وتمتاز الجريمة السيبرانية بطائفة من الخصائص التي جعلتها متفردة في صورتها عن باقي الجرائم الأخرى، بالنظر إلى مجموعة المعطيات الخاصة بها بالدرجة الأولى، سواءاً من ناحية أداء ارتكابها أو مرتكبيها، أو حتى كيفية إثباتها ومعاينتها، وتمثل تلك المعطيات بـ:

١- إن طبيعة الجرائم السيبرانية وتمييزها عن الجرائم التقليدية يرجع إلى البيئة التي ترتكب فيها الجريمة وهي الأداة أو الوسيلة التي استخدمها الجاني في ارتكاب فعله غير المشروع وتتطلب توفر معرفة أو حد أدنى من الثقافة التقنية لدى الجاني، وهي لا تخرج عن كونها سلوك إجرامي جرمه القانون وتتجه إرادة الجاني إليه، رغم وجود نص قانوني يجرم السلوك.

٢- الجريمة الإلكترونية ذات بعد دولي عابرة للحدود فهي تتجاوز الحدود الجغرافية بسبب تنفيذها عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان تحديات قانونية فنية بل سياسية بشأن مواجهتها، لا سيما فيما يتعلق بإجراءات الملاحقة الجنائية (عطايا، ٢٠١٥).

٣- صعوبة الكشف عن مرتكب الجريمة السيبرانية إلا بأساليب أمنية وتقنية عالية (العنزي، ٢٠٢٢).

أساليب الأمن السيبراني العالمي:

يشمل الأمن السيبراني وجود إستراتيجية تشمل استعراضاً عاماً أولاً لمدى كفاءة الممارسات الوطنية الحالية والنظر في دور جميع أصحاب المصلحة في هذه العملية، ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي، تحت الحكومات إلى المساعدة في عملية حماية البنية التحتية لمعلوماتها الحيوية، وتعزيز هذه الحماية وضمانها.

وتواصل الحكومات في كثير من الأحيان الاضطلاع بدور قيادي في أمن الشبكات فإن ماله أهميته الخاصة ضماناً لإدماج مضاعفة الثقة وتطوير وتطبيق السياسات، أما على الصعيد الدولي تقتضي حماية البنية التحتية للمعلومات وتعزيز الأمن السيبراني، التعاون والتنسيق بين الدول على الساحة الدولية (الشهري، ٢٠١٩).

أهم أدوات الأمن السيبراني للحماية من الهجمات الالكترونية

فيما يلي ست أدوات وخدمات حيوية يحتاج كل مدير أمن سيبراني النظر في الاستثمار فيها ضمن المؤسسة لضمان أن يكون أمنها السيبراني قوياً قدر الإمكان.

١. جدار الحماية Firewall

اعتقد أنك سمعت مسبقاً عن جدار الحماية وتفكر الآن بأن هذه الأداة قد عفا عليها الزمن نتيجة التعقيد الكبير الذي وصلت له عمليات القرصنة في يومنا هذا، لكن هذا غير صحيح! بل إن جدار الحماية يبقى من أهم أدوات الأمان، حيث يساهم هذا الجدار بشكل رئيسي بمنع أي وصول غير مصرح به إلى نظامك.

ما هو تعريف جدار الحماية؟

يعرف جدار الحماية أو ما يطلق عليه "الجدار الناري" على أنه: جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب، ويكون أداة مخصصة أو برنامج على جهاز حاسوب آخر، الذي بدوره يقوم بمراقبة

العمليات التي تمر بالشبكة ويرفض أو يسمح فقط بمرور برنامج طبقاً لقواعد معينة.

يراقب جدار الحماية حركة مرور الشبكة بالإضافة إلى محاولات الاتصال، ويقرر ما إذا كان يمكنك المرور بحرية إلى شبكتك أو جهاز الكمبيوتر الخاص بك أم لا.

أنواع جدران الحماية

يوجد عدة أنواع لجدران الحماية وهي كالآتي:

١- Proxy Firewall يعمل Proxy Firewall كبوابة دخول Gateway بين شبكة وأخرى لتطبيق معين. خوادم البروكسي يمكنها تزويد وظائف إضافية كتحزين المحتوى المؤقت Content Caching وكذلك الامن عبر منع الاتصالات المباشرة من خارج الشبكة.

يمكن أن يؤثر هذا النوع على القدرات الانتاجية وعلى التطبيقات التي يدعمها، وهو نوع قديم من الجدران النارية.

٢- Stateful Inspection Firewall هذا النوع من الجدران النارية يسمح أو يحجب حركة مرور البيانات أو الاتصالات مستنداً على بعض العوامل وهي: الحالة، الناقل، البروتوكول.

كما يعمل هذا النوع على مراقبة جميع الأنشطة منذ اللحظة الاولى لبدء الاتصال وحتى اغلاقه ويتخذ قرارات التصفية بالاستناد على القواعد التي يحددها المدير وكذلك "السياق".

ما يعنيه السياق هو: استخدام المعلومات من الاتصالات السابقة والحزم العائدة لنفس الاتصال.

٣- UTM Firewall (Unified Threat Management):

يعني الادارة الموحدة للتعامل مع التهديدات.

عادة ما يجمع جدار الـ UTM الناري بين وظائف الجدار الناري التفتيشية وبين برامج مضادات الفيروسات antivirus ، كما يمكن أن يتضمن بعض الخدمات الإضافية مثل إدارة الخدمات السحابية.

٤- Next-generation Firewall (NGFW): هي جدران نارية

متطورة ليست فقط لتصفية الحزمات او لتفتيش الحالة، توظف أغلب الشركات هذه الانواع المتطورة من الجدران النارية لحجب التهديدات الحديثة كالبرامج الضارة المتطورة والهجمات على التطبيقات.

على الرغم من كون جدار الحماية مفيداً، إلا أن له مشاكل او قيود، فهو غير فعال تماماً للتصدي لكل الهجمات، ففي يومنا هذا، لقد تعلم المتسللون المهرة كيفية إنشاء البيانات والبرامج التي تخدع جدران الحماية للاعتقاد بأنها موثوق بها - وهذا يعني أن البرنامج يمكنه المرور عبر جدار الحماية دون أي مشاكل، لكن على الرغم من ذلك، لا تزال جدران الحماية فعالة للغاية في اكتشاف الغالبية العظمى من الهجمات الالكترونية الضارة الأقل تعقيداً على عملك.

٢. برامج مكافحة الفيروسات Antivirus Software

إذا كنت تدير نشاطاً تجارياً ولم يكن لديك قدر كبير من الخبرة في مجال الأمن السيبراني، فقد تفترض أن المصطلحين "جدار الحماية" و "مكافحة الفيروسات" مترادفان، لكنهما ليسا كذلك.

من الضروري أن يكون لديك جدار حماية قوي وبرنامج مكافحة فيروسات محدث للحفاظ على نظامك آمناً، وبحال كنت مسؤولاً عن أنظمة المؤسسة فيجب تطبيق ذلك على كل الأنظمة الموجودة في المؤسسة.

ستتنبهك برامج مكافحة الفيروسات إلى الإصابة بالفيروسات والبرامج الضارة، كما سيقدم العديد منها خدمات إضافية مثل فحص رسائل البريد الإلكتروني للتأكد من خلوها من المرفقات الضارة أو روابط الويب.

٣ .خدمات البنية التحتية للمفاتيح العمومية PKI Services

ما نعني بـ PKI ؟

البنية التحتية للمفاتيح العامة هي الترتيبات التي يتم بها ربط المفتاح العام مع المستخدم بواسطة مصدر الشهادة (Certificate Authority CA) ، هوية المستخدم يجب أن تكون فريدة لكل مصدر شهادة، يتم ذلك عن طريق برمجيات خاصة في مصدر الشهادة، من الممكن ان تكون هذه البرمجيات تحت اشراف بشري، جنباً إلى جنب مع برمجيات مُنَسِّقة في مواقع مختلفة ومتباعدة.

يربط العديد من الأشخاص PKI فقط بـ SSL أو TLS ، وهي التقنية التي تقوم بتشفير اتصالات الخادم والمسؤولة عن HTTPS والقفل الذي تراه في أشرطة عناوين متصفحك.

في حين أن SSL مهم للغاية بالطبع، ليس فقط لمواقع الأمان العامة ولكن أيضاً لشبكاتك الداخلية، يمكن أن يحل PKI بالفعل عددًا من نقاط الضعف الشائعة في مجال الأمن السيبراني ويستحق مكانًا مرموقاً في مجموعة الأمان لكل مؤسسة.

بالإضافة إلى أمان الخادم، كما هو مذكور أعلاه، يمكن استخدام PKI من أجل:

تمكين المصادقة متعددة العوامل Multi-Factor Authentication والتحكم في الوصول: هنا يمكنك أن تتأكد من أن المستخدمين والآلات والأجهزة المعتمدة فقط (أولئك الذين لديهم شهادات تم تكوينها بشكل صحيح) يمكنهم الوصول إلى الشبكات الخاصة بك وتشغيلها.

قم بإنشاء توقيعات رقمية متوافقة وموثوق بها: تصادق التوقيعات الرقمية Digital signatures على هوية الموقع وتنشئ ختمًا واضحًا لحماية محتويات المستند وتلبية متطلبات الامتثال.

تشفير اتصالات البريد الإلكتروني والمصادقة على هوية المرسل: يعمل التوقيع الرقمي لجميع رسائل البريد الإلكتروني الداخلية وتشفيرها على التخفيف من مخاطر التصيد الاحتيالي وفقدان البيانات من خلال التحقق بوضوح من مصدر الرسالة حتى يتمكن المستلمون من تحديد رسائل البريد الإلكتروني الآمنة مقابل رسائل التصيد الاحتيالي والتأكد من أن المستلمين المقصودين فقط يمكنهم الوصول إلى محتويات البريد الإلكتروني.

التوقيع رقميًا وحماية التعليمات البرمجية: طمأن المستخدمين النهائيين بأن الشفرة شرعية وأنها تأتي من مصدر تم التحقق منه، واحم الكود من العبث والتهديد بإدخالات البرامج الضارة.

بناء الهوية والثقة في النظم البيئية لإنترنت الأشياء: إن منح كل جهاز / نقطة نهاية IoT هوية فريدة يعني أنه يمكنهم المصادقة عند اتصالهم بالإنترنت، وإثبات سلامتهم، والتواصل بشكل آمن مع الأجهزة والخدمات والمستخدمين الآخرين.

٤. خدمات الكشف المُدارة

نظرًا لأن مجرمي الإنترنت والمتسللين أصبحوا أكثر تعقيدًا، وأصبحت التقنيات والبرامج التي يستخدمونها أكثر تقدمًا، فقد أصبح من الضروري للشركات الاستثمار في أشكال دفاعية أكثر قوة.

في عام ٢٠١٨، لم يعد مجرد وجود دفاعات تتفاعل مع التهديدات أمرًا كافيًا - بل يجب أن تكون تلك الدفاعات استباقية وقادرة على تحديد الهجمات الإلكترونية قبل أن تتسبب في حدوث مشكلات.

شهد الأمن السيبراني تحولاً من الاستثمار في التقنيات التي تحاول منع احتمال وقوع هجوم نحو الخدمات المتقدمة التي تتفاعل مع مشكلات الأمان المحتملة وتكتشفها، وتستجيب لها بأسرع ما يمكن.

يعد تحديد الهجوم والقضاء عليه قبل انتشاره أقل ضرراً بكثير من محاولة التعامل مع هجوم له بالفعل موطئ قدم قوي على شبكة تقنية المعلومات الخاصة بك.

٥. اختبار الاختراق

يعد اختبار الاختراق طريقة مهمة لاختبار أنظمة الأمان الخاصة بشركتك.

اختبار الاختراق

أثناء اختبار الاختراق، سيستخدم متخصصو الأمن السيبراني نفس الأساليب التي يستخدمها المتسللون للتحقق من نقاط الضعف المحتملة.

يحاول اختبار (pen test) محاكاة نوع الهجوم الذي قد تواجهه الشركة من المتسللين المجرمين، بدءاً من اختراق كلمة المرور وحقق الشفرة وحتى التصيد الاحتيالي.

بمجرد إجراء الاختبار، سيقدم لك المختبرون نتائجهم ويمكنهم أيضاً المساعدة من خلال التوصية بالتغييرات المحتملة على نظامك.

٦. تدريب الموظفين

قد لا تفكر في تدريب الموظفين على أنه "أداة" ولكن في النهاية، يعد وجود موظفين على دراية بمخاطر الهجمات الإلكترونية، ويفهمون دورهم في الأمن السيبراني أحد أقوى أشكال الدفاع ضد الهجمات الإلكترونية.

هناك العديد من أدوات التدريب التي يمكنك الاستثمار فيها لتثقيف الموظفين حول أفضل ممارسات الأمن السيبراني.

يمكن أن يحدث شيء بسيط فرقاً كبيراً مثل التحديثات المنتظمة على استراتيجيات الأمن السيبراني واتباع العادات الصحيحة لاستخدام كلمات المرور، من المهم أيضاً تقديم دورات تدريبية أو عمليات محاكاة حول اكتشاف الروابط المشبوهة أو رسائل البريد الإلكتروني الاحتيالية التي قد تكون جزءاً من هجوم التصيد الاحتيالي.

لا يهم مدى قوة دفاعاتك إذا كان من الممكن خداع الموظفين من خلال تكتيكات الهندسة الاجتماعية.

مع استمرار مجرمي الإنترنت في توسيع وتطوير أساليبهم التي أصبحت أكثر تعقيداً بكثير مما مضى، فقد أصبح من الضروري لقادة المؤسسات الاستثمار في هذه الأدوات والخدمات وأي أدوات حماية أخرى للدفاع عن أنظمة مؤسساتهم.

قد يؤدي عدم القيام بذلك إلى تركك في وضع تكون فيه مؤسساتك هدفاً سهلاً للقراصنة، قد تؤدي تكلفة الاستثمار في الأمن السيبراني لترددك في تطبيق الأساليب والخدمات، ولكن عليك أن تدرك جيداً بأن هذا الإنفاق الأولي سيكافئ عملاً بالأمان والحماية على المدى الطويل، وأن تأخيرك اليوم في تعزيز واستثمار أدوات الأمن السيبراني في مؤسساتك، قد يجعل مؤسساتك غداً تواجه عواقب خطيرة جداً تجعلك تقف عاجزاً عن التعافي منها.

بحال لم تكن تعرف من أين تبدأ بعد أو ترغب بالحصول على استشارات أو تدريبات حول الأمن السيبراني، فأنت في المكان المناسب حيث تقدم لكم شركة ريناد المجد لتقنية المعلومات RMG خدمات الاستشارة والتدريب في مجال الأمن السيبراني بالتعاون مع فريقها المميز الذي يملك مئات التجارب وسنوات طويلة من الخبرة في هذا المجال، ويمكنك التواصل معنا مباشرة من هنا.

أسئلة شائعة حول أدوات الامن السيبراني للحماية من الهجمات الالكترونية

ما هو جدار الحماية Firewall ؟

هو جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب، ويكون أداة مخصصة أو برنامج على جهاز حاسوب آخر، الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يسمح فقط بمرور برنامج طبقاً لقواعد معينة.

هل تكافئ جدران الحماية برامج مكافحة الفيروسات؟

إن المصطلحين "جدار الحماية" و "مكافحة الفيروسات" ليسا مترادفين فكل منهما له وظيفة تختلف عن الآخر.

من الضروري أن يكون لديك جدار حماية قوي وبرنامج مكافحة فيروسات محدث للحفاظ على نظامك آمناً، وبحال كنت مسؤولاً عن أنظمة المؤسسة فيجب تطبيق ذلك على كل الأنظمة الموجودة في المؤسسة (حمود، ٢٠٢٤)

ما هي برامج مكافحة الفيروسات

هو برنامج يتم استخدامه لاكتشاف البرمجيات الضارة كفيروسات الحاسب، دودة الحاسوب وأحصنة طروادة وذلك لمنعها من إلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية عن طريق إزالتها أو إصلاحها.

ما المقصود بـ PKI ؟

البنية التحتية للمفاتيح العامة هي الترتيبات التي يتم بها ربط المفتاح العام مع المستخدم بواسطة مصدر الشهادة (Certificate Authority CA) ، هوية المستخدم يجب أن تكون فريدة لكل مصدر شهادة، يتم ذلك عن طريق برمجيات خاصة في مصدر الشهادة، من الممكن أن تكون هذه البرمجيات تحت إشراف بشري، جنباً إلى جنب مع برمجيات مُنَسِّقة في مواقع مختلفة ومتباعدة.

ما الذي يشير له pen test ؟

يعني اختبار الاختراق (pen test) أو ما يسمى Penetration Test وهو ممارسة تمكن المؤسسات محاكاة نوع الهجوم الذي قد تواجهه الشركة

من المتسللين المجرمين، بدءاً من اختراق كلمة المرور وحقق الشفرة وحتى التصيد الاحتيالي.

بمجرد إجراء الاختبار، سيقدم لك المختبرون نتائجهم ويمكنهم أيضاً المساعدة من خلال التوصية بالتغييرات المحتملة على نظامك.

البنية التحتية الحساسة:

يتكون الانترنت من مجموعة من الشبكات المستقلة تتصل ببعضها البعض باستخدام معايير مفتوحة لضمان إمكانية التشغيل البيئي، وكذلك تمثل البيئة التحتية لشبكة المعلومات العناصر التي تشكل وتعين على نقل البيانات القابلة للاستخدام عبر تلك الشبكات، ونظراً لاعتماد معظم اقتصادات الدول ومجتمعاتها وخدماتها الأساسية حالياً على الانترنت، فقد أصبح المحافظة على إمكانية الاتصال يمثل أولوية قصوى وفيما يلي العناصر الأساسية للبنية التحتية لشبكة الانترنت:

١. البروتوكولات والخدمات:

البروتوكولات هي معايير فنية تتيح لمختلف أنظمة الحواسيب إمكانية التواصل مع بعضها البعض، وتمثل البروتوكولات والخدمات عناصر أساسية لضمان أمن البنية التحتية لشبكة الانترنت، فبدونها لا يمكننا إرسال البيانات واستقبالها أو التنقل بين صفحات الانترنت للوصول إلى المعلومات ومشاركتها أو التواصل مع الآخرين، وتمثل مجموعة تي سي بي والاي بي التي تشكل أساس الانترنت مثالا رئيسياً على تلك البروتوكولات.

٢. البرمجيات والمعدات الحاسوبية:

وتمثل أنظمة التشغيل والبرامج الثابتة وتنطوي البرمجيات على ثغرات أمنية يجب معالجتها من خلال التحديث المنتظم وتصحيح الأخطاء وغيرها من الوسائل، ويقصد بالمعدات الحاسوبية الآلات والتوصيلات السلكية عبر أجهزة الشبكات مثل المفاتيح وأجهزة التوجيه وجدران الحماية والبوابات والخوادم والحواسيب الشخصية

والأجهزة اللوحية والهواتف النقالة، وقد يؤدي فقدان تلك العناصر الأساسية للبنية التحتية (أي الأصول والمرافق، والنظم والشبكات، والعمليات والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها) أو تعرضها لانتهاكات أمنية إلى:

- أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها، بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر إلى خسائر كبيرة في الممتلكات والأرواح، مع مراعاة الآثار الاقتصادية والاجتماعية الكبيرة.
- تأثير كبير على الأمن القومي والدفاع الوطني واقتصادها ومقدراتها الوطنية (السيراني، ٢٠١٨).

خطوات تحديد أهداف الامن السيبراني:

يعد إنشاء قدرة وطنية لإدارة الحوادث مهمة طويلة الاجل تبدأ بإنشاء مجموعة فرق وطنية للاستجابة لحوادث الأنظمة الالكترونية منها تحديد أو إنشاء قدرات وطنية ووضع أليات داخل الحكومة للتنسيق بين القطاع المدني والحكومي، ولم تنشئ أغلب الدول العربية هيئة وطنية للأمن السيبراني باستثناء بعض الدول التي بعثت مثل هذه الهيئات بتسمية مختلفة، أما في بعض الدول العربية الأخرى، فنلاحظ إحداث مجالس وهيئات عدة لها دور هام في تحديد الرؤية الاستراتيجية الوطنية للأمن السيبراني وفي وضع البرامج العملية لتحقيقها، تتخذ بعض الأحيان شكل مجالس، وفي أحيان أخرى شكل هيئات إدارية تابعة لرئاسة الجمهورية أو للوزارة المكلفة بالأمن أو الدفاع الوطني أو بالعدل، مثلما هو الشأن في مصر المتمثل في المجلس الأعلى للأمن السيبراني التابع لمجلس الوزراء، والجزائر المتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، أما في الكويت فتباشر الهيئة العامة للاتصالات وتقنية المعلومات الاختصاص المتعلق بمهام ومسؤوليات الأمن السيبراني وغيرها في مجال حماية البيانات الشخصية، نلاحظ بأن بعض الدول العربية أحدثت هيئات

وطنية لمراقبة البيانات الشخصية من ذلك الدولة التالية: تونس والامارات والمغرب ومصر والأردن، ولكن من المفيد التأكد على عدم خضوع هذه الهيئات إلى نفس النظام القانوني، وعدم تمتعها بنفس الصلاحيات والامتيازات مع الملاحظ أن هناك بعض الدول العربية التي أوكلت مهمة مراقبة البيانات الشخصية إلى مصالح وزارة مثلما هو الشأن لدولة قطر، حيث جعل المشرع من الوحدة القانونية لوزارة الاتصالات المصلحة المختصة في هذا المجال (السيراني، ٢٠٢١).

مهام إدارة البحوث والمراقبة في الأمن السيبراني:

يقع على عاتق الحكومة إنشاء أو تحديد منظمة وطنية تعمل كجهة اتصال وذلك لضمان الفضاء السيبراني والعمل على حماية البنية التحتية الحيوية للبيانات والمعلومات، تتضمن مهام هذه المنطقة المراقبة والانذار والاستجابة وجهود التعايش وتيسير التعاون بين الكيانات الحكومية والقطاع الخاص، بالإضافة إلى الدوائر الأكاديمية والمجتمع الدولي.

وركزت العديد من الدراسات على المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي وتحديد جرائم الاعتداء على الحياة الخاصة، والسب والقذف، والمسام بالقيم الدينية، وبالاتماد على تحليل قوانين مكافحة جرائم تقنية المعلومات أظهرت النتائج ان المشرع حرص في كل من عمان والكويت وقطر والامارات العربية المتحدة على تجريم الآراء على تجريم الآراء التي تؤدي إلى الفتنة بين افراد المجتمع، أو التي تمس القيم الدينية أو النظام العام في الدولة، كما جرم الاعتداء على الحياة الخاصة والسب والقذف باستخدام وسائل التواصل الاجتماعي، ويتم ذلك من خلال قانون مكافحة جرائم تقنية المعلومات في كل بلد (حسين، ٢٠١٨).

نشر خدمات الأمن السيبراني:

وفقاً لما أوردته تقارير منظمة التعاون والتنمية في الميدان الاقتصادي، فإن القوى الدافعة الرئيسية لأي ثقافة للأمن على المستوى الوطني

تتمثل في تطبيقات الحكومة الالكترونية وخدماتها، وحماية البنية التحتية الحيوية للمعلومات، ونتيجة لذلك، ينبغي للإدارات الوطنية تنفيذ تطبيقات وخدمات الحكومة الالكترونية من أجل تحسين عملياتها الداخلية وتوفير الخدمات الأفضل للقطاع الخاص والمواطنين، كعنصر مضاعف نحو تعزيز نشر ثقافة الأمن (الزبيدي، ٢٠٢١).

وكان قرار الجمعية العامة للأمم المتحدة رقم (٥٧/٢٣٩) بإرساء الثقافة العالمية للأمن السيبراني، والقرار ٥٨/١٩٩ بإرساء ثقافة عالمية لأمن الفضاء الحاسوبي وحماية البنى التحتية الحيوية للمعلومات والبيانات قرارا يروج لثقافة الأمن السيبراني على مستوى الأشخاص والدول، وذلك عن طريق توعية القطاع الخاص والمجتمع المدني والافراد بتأمين تشغيل واستخدام البنية التحتية للمعلومات، بما في ذلك المعلومات والبيانات الحكومية، ويشتمل ذلك على تدريب مستخدمي الشبكات في الأنظمة الحكومية والخاصة، مع إدخال تحسينات مستقبلية على الجوانب الأمنية، فيجب اعتماد الدول من خلال أنشطتها التعاونية على نهج متعدد التخصصات ومتعدد أصحاب المصلحة لتنفيذ عملة الامن التي يقوم بعضها بإنشاء هيكل إدارة رفيع المستوى لتنفيذ السياسات الوطنية، كما يكتسي التعاون الدولي أهمية بالغة في تعزيز تلك الثقافة، جنباً إلى جنب مع دور المنظمات الإقليمية في تيسير التفاعلات والتبادلات الدولية وتوعية المستخدمين ومسؤوليتهم تجاه القضايا الرئيسية (طوال، ٢٠٢٤).

مسئولية مقدمي خدمات الامن السيبراني

يشهد العالم جملة من التغيرات والتطورات والتحولات في كافة مناحي الحياة وتؤثر بدورها على عمل مؤسسات القطاعين العام والخاص على حد سواء شأنها في ذلك شأن مختلف قطاعات المجتمع، ولعل ابرز هذه التغير تتمثل في تطور تكنولوجيا الاتصالات وتقنية المعلومات والشبكة العالمية الانترنت التي ساهمت في إحداث تغير ملحوظ في عمليات القطاعين العام والخاص على حد سواء، ووفقاً لأهمية جودة الخدمات الالكترونية ودورها الهام في تسهيل وتسريع

العمليات والخدمات، فلم يعد هناك حاجة للوقوف والانتظار طويلا للحصول على خدمة أو معاملة، وهذا أدى إلى توفير الوقت والجهد والتقليل قدر الإمكان من الموارد المستهلكة في مؤسسات في حالة الخدمات التقليدية (عبدالقادر، ٢٠١٧).

يضاف إلى ذلك ما تقدمه الانترنت من إمكانيات وقدرات للمجالات العلمية والثقافية والخدماتية، حيث تسمح بالوصول إلى مناطق بعيدة، وإلى فئات محددة، ككبار السن والمرضى وغيرهم من ذوي الاحتياجات الخاصة، هذا عدا عن الدور الذي يمكن أن تؤديه في تبادل المعلومات، في أوقات الأزمات الإنسانية والكوارث، بحث تتأمن المساعدات وتوزع بالسرعة المطلوبة، ولا تقف الأبعاد الاجتماعية عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والإفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير نشاطاته المختلفة، بل تتعداها إلى صيانة القيم الجوهرية في المجتمع، كالانتماء والمعتقدات، بالإضافة إلى العادات والتقاليد عبر إنشاء المجموعات التي تهتم بنشر الوعي حول هذه المسائل.

إن الحقيقة الواضحة أمامنا تقودنا إلى القول بأن هذا الجدل لا يمكن أن يؤدي بأي شكل من الأشكال إلى استبعاد مسئولية مقدمي الخدمات، بحيث يصبح الممنوع مشروعاً، والواقع ان المسئولية يمكن ان تجد أسساً مختلفة مثل الإخلال بالالتزام العقد أو انتهاك حقوق الملكية الفكرية، أو عن طريق إفشاء اسرار مهنية، أو المساس بحرمة الحياة الخاصة، أو عبارات السب والقذف، فإزاء هذه المخالفات المتعددة يثور التساؤل حول الطريقة الأنسب لمعالجتها (ابراهيم، ٢٠١٨).

فهل من الأمثل الأخذ بعين الاعتبار خصوصية بعض المخالفات، كتلك المتعلقة بحقوق الملكية الفكرية مثلاً، وبالتالي تخصيص النصوص القانونية لمعالجة كل مخالفة وحدها؟ أم من الأفضل وضع قواعد عامة للمسئولية المرتكبة على الأمن السيبراني بصرف النظر عن مضمونها، ويمكن للمسئولية في مقدمي الخدمات الأمنية السيبرانية أن

تجد أسساً مختلفة مثل الإخلال بالالتزام العقدي أو انتهاك حقوق الملكية الفكرية، فإزاء هذه المخالفات المتعددة يثور التساؤل حول الطريقة الأنسب لمعالجتها، وساعد التقدم الكبير في مستوى التقنية المعلوماتية في توظيف هذه التقنية من أجل تسهيل الولوج إليها ولهذه الاعتبارات فإن الفقه والقضاء المقارن يرى أن من شأن زيادة استخدام التقنيات الرقمية يظهر الاحتياج إلى قانون جديد للإجراءات الجنائية يختلف في قواعده عن القوانين المطبقة حالياً (توفيق، ٢٠١٩).

وتمثل خدمات الخصائص الوظيفية التي تجعل من الانترنت أداة جذابة ومفيدة من خلال تيسير عملية تبادل المحتوى عبر الانترنت، وتتضمن خدمات التحتية لشبكة الانترنت "العنونة" وهو النظام العالمي لتحليل أسماء النطاقات التي يستخدم نظام أسماء النطاقات (DNS)، والذي يتيح لنا التنقل بين صفحات الانترنت، وتشمل وظائف مثل التوجيه واستخدام بروتوكول البوابة الحدودية (BGP)، وخدمات التطبيقات مثل الشبكة العنكبوتية العالمية (الطويل، ٢٠١٥).

ماهية مزودي خدمات الاتصالات الالكترونية:

مزود الخدمة أو متعهد الوصول هو الموزع لخدمة الانترنت، والذي يتيح من خلال حاسباته المتصلة بالشبكة للمستخدمين الوصول إلى خدمة الانترنت، وتوصيل المستخدم بالمواقع التي يرغب في الوصول إليها، ويمكن لمزودي خدمات الانترنت توفير خدمات أخرى كتخزين البيانات عن بعد لعملائهم، ويمكن تداخله إذا لاحظ مخالفات تشكل جرائم يعاقب عليها القانون، يتضح من ذلك أن مقدمي خدمات الانترنت لا يقدموا المعلومات، إنما يحققوا اتصال الغير بالشبكة فقط ليس إلا، وليس له سيطرة على المادة محل البحث، لكن يمكن تدخله لقطع هذا الاتصال إذا لاحظ مخالفات تتعلق بتلك المادة محل البحث أو المنشورة، ومن الناحية الفنية فيربط مقدمي الخدمات بزبائنه باستخدام تقنية نقل البيانات لنظام الانترنت مثل الاتصال الهاتفي، وخط المشترك الرقمي للاتصال، وكابل المودم ولاسلكية الوصلات المخصصة عالية السرعة، وهو يوفر حسابات البريد الالكتروني

للمستخدمين والتي تسمح لهم بالتواصل مع بعضهم البعض، عن طريق ارسال واستقبال الرسائل الالكترونية من خلال مزود الشبكة وكجزء من خدمة البريد الالكتروني ما يوفر مزود الخدمة و عميل البريد الالكتروني حزمة البرامج التي طورت داخلياً أو خارجياً عن طريق ترتيب عقد خارجي، كما يمكن لمزودي خدمات الانترنت توفير خدمات أخرى كتحزين البيانات عن بعد لعملائهم (ابراهيم، ٢٠١٨).

مما سبق يتضح أن متعهد توصيل الخدمة هو الشخص الطبيعي او الاعتباري الذي يملك خدمة الاتصال مباشرة بالشبكة الدولية للمعلومات، وتقتصر المهمة لديه على تمكين الافراد الذين يبرمون عقداً معه من الاتصال بالشبكة للاطلاع على مختلف المواقع من أجل الوصول إلى خبر أو معلومة معينة، فهو لا يقدم المعلومات ولكنه يحقق اتصال الغير بالشبكة، وليس له سيطرة على المادة محل البحث ولكن يمكن تداخله إذا لاحظ مخالفات تتعلق بمحتوى المادة التي يتم بثها، أو إذا كانت تشكل جرائم يعاقب عليها القانون (حجازي، ٢٠١٩).

التزامات مقدمي خدمات الانترنت:

- ١- يجب على مزودي الخدمة في حالة نشر أي بيانات أو معلومات من شأنها تهديد الأمن القومي أو الاقتصادي للدولة أو نشر المواد الإباحية أو التحريض على الاتجار بالبشر، وجميع الأنشطة غير القانونية، ابلاغ السلطات بعناوين هؤلاء الأشخاص والبريد الالكتروني والصفحة الشخصية، الأمر الذي يتعين معه إلزام مزودي الخدمات مدير تحرير الموقع بالحصول على المعلومات الشخصية للمستخدمين مسبقاً عند إنشاء صفحات التواصل.
- ٢- يتلزم مقدمي الخدمة باحترام الحق في الخصوصية وسرية المراسلات.
- ٣- يجب على مقدمي الخدمة مراقبة المعلومات التي تشكل جريمة تهدد سلامة أمن الدولة، وإبلاغ السلطات المختصة عنها.

- ٤- إذا ورد بلاغ لمقدمي الخدمة كالنشر أو بيانات غير قانونية يتعين عليهم الامتناع عن تخزينها.
- ٥- عدم جواز نسخ أي بيانات أو نقلها إلى الجمهور دون موافقة أصحاب حقوق الطبع والنشر.
- ٦- عدم جواز إلغاء أو حذف أو تعديل أو تدمير أو إفشاء أو إتلاف أو تغيير أو عادة نشر بيانات أو معلومات.
- ٧- يتلزم مقدمي الخدمة بتقديم بيانات عملائهم إلى سلطات التحقيق إذا طلب منه ذلك، وعدم فتح إي اشتراك لأي عميل دون الحصول على بيانات تحقيق شخصيته، ويترتب على الإخلال بهذا الالتزام انعقاد المسؤولية الجنائية لمقدمي خدمة الانترنت (توفيق، ٢٠١٩).

حماية الأنظمة الالكترونية:

ساهم التطور التكنولوجي في مجال الاتصالات وتقنيات المعلومات في سرعة انتشار المعلومات وسهولة تداولها عبر خدمات الانترنت، مما أدى إلى ظهور العديد من المخاطر والاعتداءات التي تتم في الأنظمة الالكترونية، الأمر الذي أدى إلى ضرورة نشر الوعي بين المستخدمين لحماية أمن المعلومات، وذلك من خلال قيام الدول والمنظمات إلى وضع التشريعات التي تحمي أمن المعلومات، فضلا عن العديد من المنظمات التي تقوم بوضع مواصفات دولة لتكون بمثابة الدليل الاسترشادي الأمثل لحماية أمن المعلومات مثل منظمة الايزو (جوهري، ٢٠٢٣).

ويرتبط الامن السيبراني ارتباطا وثيقا بالتحول والتبادل الرقمي للبيانات، لكف الملف للنظر والمؤسف سهولة اختراق تلك المعلومات والبيانات، والاعتداء عليها والعبث بها، وتقف الدول عاجزة عن منعها أو الوقاية منها، كون التقنية المستخدمة في هذه الجرائم متطورة جداً، مما يتطلب ضرورة العمل والحرص على حماية أمن تلك المعلومات والبيانات المتوفرة على مختلف الأنظمة، لأن فقدان المعلومات والبيانات المنتقلة عبر الشبكات الالكترونية من الأمور المكلفة الصعب تعويضها، كما أن حماية تلك المعلومات والبيانات فيه

حافضة على النفس والاعراض والأموال المرتبطة بهذه البيانات والمعلومات.

وتعتبر الجرائم الالكترونية ظاهرة إجرامية جديدة مستحدثة تدق اجراسها لتنبئ المجتمع المعاصر بمدى وحجم المخاطر وهول الخسائر الناجمة عن تلك الجرائم التي تمثل اعتداء صارخ على التقنيات الحديثة بكافة معطياتها من بيانات ومعلومات وبرامج على اختلاف أنواعها (عوض، ٢٠٢٢).

الجريمة السيبرانية كتهديد للأمن السيبراني:

أدى التقدم العلمي والتقني في مجال الاتصالات وظهور شبكة الانترنت وتضخمها وامتدادها إلى كل أقاليم الدول تقريباً إلى تنوع وتعدد الأنشطة الاجرامية التي ترتكب من خلالها وعبر عدة دول، كما أفرزت المواقع الالكترونية ثورة إعلامية، أثبتت أهميتها في ساحات التغيير، حتى إنها نافست الاعلام التقليدي، دوراً وحضوراً، كما أثارت إشكالات عديدة على الصعيد القانوني، أهمها التساؤل عن مسئولية المواقع الالكترونية الإعلامية جنائياً، عن محتواها الضار أو غير المشروع، ومع كثرة الأشخاص القائمين على عمل هذه المواقع يثار التساؤل عن تحديد المسئول جنائياً وكذلك الحالات التي تقوم فيها المسئولية الجنائية للمواقع الالكترونية، كما أدى ظهور الجرائم السيبرانية كنمط جديد من أنماط الجريمة إلى توجه المجتمع الدولي للتعاون من أجل تصد دماغ لتلك الجرائم التي لها بالغ الأثر السلبي، حيث تعتمد أغلب المجتمعات على تقنيات الاتصالات والمعلومات، ومع ذلك الاعتماد المستمر تصاحبه مخاطر ناشئة ومحتملة تهدد تلك الشبكات، وتؤثر بالسلب على البنية التحتية للمعلومات الوطنية الحساسة، وخاصة المعلومات الشخصية والأمن الفكري (الزهراني، ٢٠٢٣).

وتصف الجريمة المتعلقة بالمعلومات الحاسوبي بأنها فعل إجرامي هدفه المعلومات المحاسبية، بينما تصف اتفاقية منظمة شنغهاي

للتعاون على نطاق أوسع جرائم المعلومات بأنها استخدام موارد المعلومات والتأثير عليها في الفضاء المعلوماتي لأهداف غير مشروعة، أما اتفاقية مجلس أوروبا على الرغم من تعريفها للمصطلحات فإنها تستخدم عناوين تجريم واسعة، تشتمل على جرائم ضد سرية وسلامة وتوافر البيانات والمعلومات والأنظمة الالكترونية، أما مشروع قانون الاتحاد الأوروبي فيستخدم على نحو مشابه عناوين تجريم تميز بين جرائم خاصة بتكنولوجيات المعلومات والاتصال وجرائم ذات تكييف قانوني محلها تكنولوجيات المعلومات والاتصال، وفي الواقع تتبنى بعض الصكوك الدولية والإقليمية المعنية بالجريمة السيبرانية مفهوماً ضيقاً للأنظمة أو البيانات الحاسوبية لتكون محل الجريمة، في حين أن الصكوك الأخرى تتنازل نطاقاً عريضاً من الجرائم، تتضمن أفعالاً حيث يكون محل الجريمة شخصاً أو شيئاً ما ذو قيمة، أو بالأحرى نظام حاسوبي أو بيانات حاسوبية، ولكن أينما يعتبر نظام حاسوبي أو نظام معلومات فإنه جزء لا يتجزأ من أسلوب ارتكاب الجريمة (المري، ٢٠٢٤).

الأفعال التي تشكل الجريمة السيبرانية:

تركز الفئة الثانية على الأفعال التي يعتبر فيها النظام الحاسوبي بمثابة الأسلوب الأساسي المستخدم في ارتكاب الجريمة، ويصاحب ذلك اختلاف في محل هذه الأفعال الاجرامية، ففي حالة الاحتيال باستخدام الكمبيوتر تعتبر المقتنيات الاقتصادية محل الجريمة، أما في حالة جرائم حقوق المؤلف والعلامات التجارية المرتكبة بواسطة الحواسيب، فإن محل الجريمة يتمثل في حقوق الملكية الفكرية المحمية.

ومن هذه التهديدات والتسلط ما قامت به العديد من شركات البرمجيات رفيعة المستوى عام ٢٠١٠ من الابلاغ عن سلسلة من الهجمات عبر الانترنت، وفي النهاية قد سجلت اختراقات في محرك بحث لشركة كبيرة، وباستخدام نقطة ضعف في أحد متصفحات شبكة الانترنت، قام المهاجمون بعمل نفق داخل شبكة داخلية عبر حواسيب

عمل الموظفين، المعرضة للخطر، وتمكنوا من الدخول إلى حسابات البريد الإلكتروني واختراق مركز تخزين شفرة المصدر المؤمنة على نحو غير ملائم، وفي نفس العام تلقى مستخدمو مواقع التواصل الاجتماعي رسائل بريد إلكترونية من حساب وهمي مع روابط لنظام تسجيل دخول زائف ليبدو أنه مرسل من الشركة، وبالفعل قام المستخدمون الضحايا بالدخول والتسجيل، وأصبحت وثائق المستخدمين عرضة للخطر، ومن المحتمل أن يصبح المضيف المخترق أحد الأعضاء في شبكة البوت نت، وفي أوائل عام ٢٠١٣ اتهمت النيابة العامة الأمريكية ثلاثة رجال أوروبيين بإنتاج وتوزيع فيروس حاسوبي الحق الضرر بأكثر من مليون جهاز حاسوب على مستوى العالم، وتمكنوا من الوصول إلى معلومات بشأن حسابات بنكية شخصية استولوا من خلالها على مبلغ خمسون مليون دولار أمريكي على الأقل في الفترة ما بين ٢٠٠٥ إلى ٢٠٠١، وقد تم إنتاج هذا الفيروس في أوروبا ثم انتشر في أمريكا الشمالية حيث ألحق الضرر بأجهزة الكمبيوتر التي تخص هيئات وطنية، وقد وصفت القضية بأنها واحدة من أكثر عمليات الدمار المالي التي لم تشهد مثلاًها حتى الآن (البوغانمين، ٢٠١٩).

أما الفئة الأخيرة من أفعال الجريمة السيبرانية فتتمثل في تلك المتعلقة بالمحتوى الحاسوبي، وتتمثل في الكلمات والصور المرسلات أو المخزنة والاصوات، حيث يعتبر الهدف المادي للعمل الاجرامي في الجرائم المتعلقة بالمحتوى في أغلب الأحيان هو شخص ما، أو جماعة محددة من الأشخاص أو شيء ما ذا قيمة كبيرة، أو عقيدة ما، وبنفس النهج كما في الفئة الثانية، يمكن من حيث المبدأ ان ترتكب هذه الأفعال بدون الاتصال بالإنترنت، فضلاً عن استخدام نظم حاسوبية في ذلك، واتخاذ جميع التدابير اللازمة لحماية المستخدمين سواء كانوا افراداً أو ودلاً على حد سواء (محمود، ٢٠٢٠).

التدابير الأمنية أمن المعلومات:

يهدف الأمن السيبراني بشكل مباشر إلى الانتقال من العمل التقليدي إلى استخدام التقنيات الحديثة بعمليات الاطلاع على الوثائق وكذلك الاتصالات اللازمة لممارسة العمل الرقابي، تقوم على ربط الوحدات التنظيمية التنفيذية مع الأجهزة الرقابية في التشكيلات التي تعتمد على رقابتها لتسهيل الحصول على البيانات والمعلومات بسرعة ودقة مرتفعة، والتي تهدف إلى حماية الفضاء السيبراني المحلي من خلال توافر تمكين الخصوصية وحماية سرية المعلومات، ومن هذه التدابير ما يلي:

- التدابير التنظيمية والمادية: هدفها بناء بيئة آمنة للمعلومات ومنع الوصول إلى المعلومات وقواعدها.
- التدابير التقنية: التشفير وينقسم إلى تشفير المتماثل / تشفير المفتاح الخاص (جوهري، ٢٠٢٣).

التدابير الأمنية لأمن المعلومات في المملكة (الضوابط الأساسية للأمن السيبراني):

استهدفت رؤية المملكة العربية السعودية 2030 التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه وعيشهم الكريم، ولقد كان من الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية؛ بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي الشبكات العالمية المتجددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ويتماشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتواصلها، وبما يهيئ للتعامل مع معطيات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة.

إن هذا التحول يتطلب انسيابية المعلومات وأمنها وتكامل أنظمتها، ويستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية، وتعزيزه، حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية؛

لذلك أتى تأسيس الهيئة الوطنية للأمن السيبراني والموافقة على تنظيمها بموجب الأمر الملكي الكريم رقم ٦٨٠١ وتاريخ ١٤٣٩/٢/١١ هـ، وجعلها الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه.

لقد جاءت مهمات هذه الهيئة واختصاصاتها ملببةً للجوانب الاستراتيجية، ولجوانب وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني وتعميمها على الجهات.

كما جاءت ملببةً لجوانب التحديث ومتابعة الالتزام من قبل الجهات الحكومية وغير الحكومية بما يعزز دور الأمن السيبراني وأهميته والحاجة الملحة التي ازدادت مع ازدياد التهديدات والمخاطر الأمنية في الفضاء السيبراني أكثر من أي وقت مضى.

وقد نص التنظيم المشار إليه أن مسؤولية هذه الهيئة لا يُخلى أي جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني، وهو ما أكدته الأمر السامي الكريم رقم ٥٧٢٣١ على جميع الجهات «١٤٣٩ هـ بأن ١١/ وتاريخ ١٠ الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير وضوابط وإرشادات بهذا الشأن».

ومن هذا المنطلق، قامت الهيئة الوطنية للأمن السيبراني بتطوير الضوابط الأساسية للأمن السيبراني لوضع الحد الأدنى من متطلبات الأمن السيبراني في الجهات الوطنية التي تدرج تحت نطاق عمل هذه الضوابط. وتوضح هذه الوثيقة تفاصيل هذه الضوابط، وأهدافها، ونطاق العمل وقابلية التطبيق، وآلية الالتزام ومتابعته.

وعلى مختلف الجهات الوطنية تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط، تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في

تنظيم الهيئة الوطنية للأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم (٥٧٢٣١) وتاريخ ١٠/١١/١٤٣٩هـ.

الضوابط الأساسية للأمن السيبراني في المملكة العربية السعودية:

قامت الهيئة الوطنية للأمن السيبراني (ويشار لها في هذه الوثيقة بـ "الهيئة") بتطوير الضوابط الأساسية للأمن السيبراني بعد دراسة عدة معايير وأطر وضوابط قامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية)، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة، وبعد الاطلاع على أفضل الممارسات والتجارب في مجال الأمن السيبراني والاستفادة منها، وتحليل ما تم رصده من حوادث وهجمات سيبرانية على مستوى الجهات الحكومية وغيرها من الجهات الحساسة، وبعد استطلاع آراء العديد من الجهات الوطنية وأخذ مرئياتها، وتتكون هذه الضوابط من:

- خمس مكونات أساسية (Main Domains) لضوابط الأمن السيبراني.
 - تسع وعشرون مكوناً فرعياً (Subdomains) لضوابط الأمن السيبراني.
 - ١١٤ ضابطاً أساسياً (Controls) للأمن السيبراني.
- كما أن هذه الضوابط مرتبطة مع المتطلبات التشريعية والتنظيمية الوطنية والدولية ذات العلاقة (السيبراني، ٢٠١٨).

أهداف الضوابط الأساسية للأمن السيبراني في المملكة العربية السعودية:

تهدف هذه الضوابط إلى توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني المبني على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات (Threats) الداخلية والخارجية، وتتطلب حماية الأصول المعلوماتية والتقنية للجهة التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومات.

- سلامة المعلومات.
 - توافر المعلومات.
- وتأخذ هذه الضوابط بالاعتبار المحاور الأربعة الأساسية التي يركز عليها الأمن السيبراني وهي:
- الاستراتيجية.
 - الأشخاص.
 - الإجراء.
 - التقنية.

نطاق العمل:

تُطبَّق هذه الضوابط على الجهات الحكومية في المملكة العربية السعودية (وتشمل الوزارات والهيئات والمؤسسات وغيرها) والجهات والشركات التابعة لها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة أو تقوم بتشغيلها أو استضافتها، ويشار لها جميعاً في هذا الوثيقة بالجهة، كما تشجع الهيئة الجهات الأخرى في المملكة وبشدة على الاستفادة من هذه الضوابط لتطبيق أفضل الممارسات فيما يتعلق بتحسين الأمن السيبراني وتطويره داخل الجهة.

قابلية التطبيق:

تم إعداد هذه الضوابط بحيث تكون ملائمة لاحتياجات الأمن السيبراني لجميع الجهات والقطاعات في المملكة العربية السعودية بتنوع طبيعة أعمالها، ويجب على كل جهة الالتزام بجميع الضوابط القابلة للتطبيق عليها.

من الأمثلة على الضوابط التي تتفاوت فيها قابلية التطبيق من جهة إلى أخرى حسب طبيعة أعمال الجهة واستخدامها للتقنيات المذكورة:

- الضوابط ضمن المكون الفرعي رقم (٤-٢) المتعلقة بالأمن السيبراني للحوسبة السحابية والاستضافة تكون قابلة للتطبيق وملزمة على الجهة التي تستخدم حالياً خدمات الحوسبة السحابية والاستضافة أو تخطط لاستخدامها.

- الضوابط ضمن المكون الرئيسي رقم (٥) المتعلقة بالأمن السيبراني لأنظمة التحكم الصناعي تكون قابلة للتطبيق وملزمة على الجهة التي تستخدم حالياً أنظمة التحكم الصناعي أو تخطط لاستخدامها.

مفهوم أمن نظم المعلومات

فإنه يعد مجموعة الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات فضلاً عن الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال (Warman، ٢٠١٣).

وفي تعريف (صالح، ٢٠٢٠) أنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها سواء كانت هذه المخاطر داخلية أو خارجية وذلك من خلال توفير الأدوات والوسائل اللازمة لحمايتها والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي اشخاص غير مخولين.

وتتعرض نظم المعلومات الالكترونية للكثير من المخاطر والتهديدات ومنها التلاعب في البيانات بقصد تدميرها سواء بالحذف أو بالدمج غير الصحيح لبعضها، أو بخلطها ببيانات أخرى غير حقيقية أو تبويبها بشكل خاطئ تفقد معه مدلولها ومعناها وقد يحدث التلاعب في البيانات بشكل يجعلها لا تعبر عن الحقائق التي نتجت عنها أصلاً، كما أن هذا التلاعب يحدث في مراحل مختلفة من النظام حيث المدخلات أو التشغيل أو التخزين أو المخرجات، ومن الممكن أن تكون تلك التهديدات في شكل سرقة وقت أجهزة الكمبيوتر واستخدامه في الأغراض الشخصية والدخول غير المصرح به للنظم والشبكات وتخريب وتدمير بعض الملفات، فزل النظام وسقوط شبكة الاتصال، منع الأشخاص المخول لهم بالدخول إلى النظام، الكوارث الطبيعية مثل الحرائق والفيضانات أو انقطاع مصدر الطاقة، الكوارث غير الطبيعية مثل الحرائق المفتعلة وغيرها، إدخال فيروسات للكمبيوتر، الاظهار غير المرخص به للبيانات عن طريق عرضها على شاشات

العرض أو طبعها وتوزيعها بواسطة اشخاص غير مصرح لهم بذلك، وكذلك مقاطعة تحويل البيانات من أماكن بعيدة (شحاته، ٢٠١٢).

إدارة أمن المعلومات هي نهج أمني مستمر ومنظم لإدارة حماية معلومات المنظمة من التعرض للخطر من قبل الأطراف غير المسؤولة و لضمان بقاء المعلومات آمنة فغالبا ما يواجه أمن المعلومات بالعديد من المشاكل سواء في الاجل الطويل او الاجل القصير، وقد تركز معظم منظمات الاعمال على منع حدوث مشاكل أمن المعلومات في الاجل القصير دون الاهتمام بمدى خطورة مشاكل الاجل الطويل، لذا يجب على الإدارة وضع خطة طويلة الاجل لمنع حدوث أي تهديد لأمن المعلومات في الأجل الطويل وتخفيض آثارها السلبية على المنظمة إلى أدنى حد ممكن في حالة حدوثها، كما يجب عليها تحديد نوع القضايا الهامة التي تواجه أمن المعلومات وأن تدرسها بعناية وتفهم طبيعة المشاكل المتعلقة بكل قضية حتى تستطيع تجنب تلك المشاكل في المستقبل وتقديم حلول مناسبة لها (شحاته، ٢٠١٢).

مفهوم أمن المعلومات:

هو حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل، أو من أي خطر يهددها مثل وصول أي شخص غير مخول للوصول إليها والعبث ببياناتها والاطلاع عليها، وذلك من خلال توفير الوسائل والطرق اللازمة لحمايتها من المخاطر الداخلية والخارجية، وموضوع أمن المعلومات هو موضوع قديم، ولكن زادت الحاجة والطلب عليه مع انتشار استخدام الإنترنت والاعتماد عليه في كافة مجالات الحياة، مما تطلب نقل البيانات والمعلومات عبر الشبكات المتعددة، كما أتاح انتشار شبكات التواصل الاجتماعي الملحة (دعوع، ٢٠١٦).

ولإدارة امن المعلومات مجموعة من المتغيرات الداخلية التي تعمل على نجاح برامج أمن نظم المعلومات وهذه المتغيرات هي:

١- سياسة امن المعلومات:

سياسة امن المعلومات هي مزيج من المبادئ والأنظمة والمنهجيات والتقنيات والأدوات التي أنشئت لحماية المنظمة من التهديدات، ويرى

(Tryfonas، ٢٠٠١) انها وثيقة استراتيجية بمعنى أنها تنشأ قبل القيام بأي نشاط من أنشطة أمن المعلومات فهي تتكون من الأهداف والاتجاهات والقواعد التي يجب وضعها واتباعها من قبل الموظفين والأطراف الأخرى التي تتعامل مع المنظمة، لذا يجب أن تكون هذه السياسة واضحة في تحديد الأهداف والأدوار ومسؤوليات الموظفين والأطراف الأخرى ذات المصلحة، كما يجب أن تكون شاملة بمعنى أنها تغطي جميع جوانب متطلبات وضوابط أمن المعلومات وأن تكون متناسقة مع سياسة المنظمة ورؤيتها، وتمثل سياسة أمن المعلومات حجر الزاوية في إدارة أمن المعلومات الجيدة كما أن هذه السياسة ليست ثابتة أي يجب أن يتم مراجعتها بانتظام على الأقل مرة واحدة في السنة للتأكد من أنها ذات صلة باحتياجات الوقت الحاضر ويتم إرسالها إلى كامل الموظفين والأطراف الأخرى ذات المصلحة مع مراعاة أنه عند قيام المنظمة بإحلال أساليب أمن تكنولوجية حديثة بدلاً من أساليب أمن المعلومات التقليدية يجب المفاضلة من حيث درجة الاستفادة ونجاح برامج أمن المعلومات بين البقاء على الأساليب التقليدية لأمن المعلومات مع تكاملها مع أساليب أمن المعلومات الحديثة أم الاحلال التام أكثر إفادة.

وينبغي لسياسة أمن المعلومات على المستوى المؤسسي أن تعالج أساسيات هيكل إدارة أمن المعلومات في المنظمة بما في ذلك أدوار ومسؤوليات أمن المعلومات، بيان خط الأساس للضوابط الأمنية وقواعد تجاوز خط الأساس، وقواعد السلوك التي من المتوقع أن يتبعها مستخدمو المنظمة والحد الأدنى من العواقب المترتبة على عدم الامتثال، وفيما يلي بعض المعايير التي ينبغي على المنظمة اتباعها من أجل تنفيذ سياسة أمن فعالة:

١. يجب أن تكون سياسة أمن المعلومات واضحة ومفهومة من قبل جميع الأطراف المعنية وان يتم متابعة هذه السياسة بانتظام لمعرفة ما إذا كان يتم انتهاكها كما يجب وجود مبادئ توجيهية إجرائية محددة بشكل جيد للتعامل مع حوادث انتهاك السياسة.

٢. أن تكون ملائمة للثقافة التنظيمية، وملائمة للنمط الذي يتسق مع أسلوب الاتصال العام في المنظمة.

٣. استخدام لغة بسيطة لضمان سهولة فهمها، وتحديد الغرض من السياسة ونطاق المنظمة وشرح ما هو النشاط المقبول وما هو غير مقبول.

٤. ينبغي وضع سياسة أمن المعلومات على أساس الاحتياجات الأمنية والاهداف التجارية للمنظمة.

٢- إجراءات أمن المعلومات

يرتبط أمن المعلومات بمجموعة من الإجراءات المصممة لحماية المعلومات فالإجراءات هي المبادئ التوجيهية لتنفيذ العمليات والأنشطة القائمة على أساس الاحتياجات الموضحة في سياسة أمن المعلومات بمعنى أنها إرشادات التشغيل التي تشرح كيفية تنفيذ سياسة أمن المعلومات حيث يتم اشتقاق الإجراءات من سياسة الأمن وذلك لضمان تنفيذ ISM بشكل مناسب وصحيح، كما يجب أن تكون الإجراءات واضحة ومحددة في وصف الخطوات اللازمة لإنجاز العمليات والأنشطة وينبغي استعراضها بطريقة دورية أو عند تغيرات بيئة الأمن نتيجة التطورات التكنولوجية المستمرة لذلك فإنه من الضروري وجود إدارة مسؤولة عن إدارة برنامج التغيير وقادرة على رسم إجراءات وخطوات ملائمة لإدارة ذلك التغيير حيث إنه قبل إجراء أي تغيير لابد من وضع تخطيط جيد يضمن أن اقتناء التكنولوجيا الجديدة لن يؤثر سلباً على سلامة أمن المعلومات ومدى الاستفادة منها.

٣- فريق إدارة أمن المعلومات

يتكون فريق إدارة أمن المعلومات من الموظفين المشاركين في معظم أنشطة أمن المعلومات، حيث يجب أن يتمتع هذا الفريق بالمعرفة والمهارات الواسعة والتعاون في تنفيذ عمليات ISM وأن يكون دائم التحديث مع القضايا الأمنية الحالية، كما ينبغي أن يمتلك المهارة التقنية التي تؤهله للقيام بالأعمال والمهام الجديدة.

٤- فريق تنسيق إدارة أمن المعلومات

يعمل فريق تنسيق إدارة أمن المعلومات كحلقة وصل بين كل من الإدارة العليا وفريق ISM ومراجعي أمن المعلومات والموظفين فهو المسئول عن تنظيم التدريب والتوعية بالبرامج وإدارة الموارد المالية والبشرية وتقديم تقرير عن التقدم في ISM إلى الإدارة العليا، كما ينبغي أن يتوافر في أفراد فريق التنسيق مهارات التواصل الجيدة مع الآخرين والمعرفة الكاملة بأنشطة ISM حيث القدرة على التواصل بفعالية مع جميع المستويات في المنظمة.

٥- فريق مراجعة أمن المعلومات هو فريق مسئول عن ضمان ضوابط الرقابة، وأن يتم تنفيذ العمليات والإجراءات والأنشطة بشكل صحيح، فينبغي أن يتمتع هذا الفريق بمهارات الاتصال الجيدة والالتزام بالوقت المحدد لإنهاء عملية مراجعة أمن المعلومات، ولكي يتم نجاح برامج أمن المعلومات يجب أن يكون لدى فريق مراجعة أمن المعلومات فهم جيد لعمليات ISM حيث ان نقص المعرفة قد تؤدي إلى طرح الأسئلة بطريقة خاطئة وبذلك وجود معلومات مغلوبة.

٦- تقييم إدارة أمن نظم المعلومات

يتم تقييم إدارة أمن نظم المعلومات من خلال:

الإدارة المستمرة للأعمال (خطة استمرارية الاعمال): الشيء المهم في استمرارية الاعمال هي خطة استمرارية الاعمال، لذلك يجب على المنظمة تحديد متطلبات أمن المعلومات وجعلها جزء لا يتجزأ من خطة استمرارية الاعمال، وأن تقوم المنظمة أيضا بتحديد خطة العمليات والإجراءات والموارد والمسئوليات للسيطرة على الحوادث والكوارث ولضمان استمرارية الاعمال أثناء الاحداث غير المقصودة وبعدها، ينبغي تطوير هذه الخطة وتوثيقها والموافقة عليها من قبل الإدارة كما يجب اختبارها لمراقبة فعاليتها (صالح، ٢٠٢٠).

برامج أمن المعلومات:

يرى البعض أنه لا يكفي أن يكون لدى المنظمة بعض سياسات الأمان والتركيز فقط على تأمين الشبكة الخاصة بها، حيث أنه لدمج الأمان في العمليات التجارية، تحتاج المنظمة إلى برنامج قوي لأمن

المعلومات يقوم بتعيين المحركات التجارية ومتطلباتها القانونية والتنظيمية والمخاطر والتهديدات التي تتعرض لها، لذلك من الضروري معرفة ما يلي

- مفهوم ومكونات برامج امن المعلومات:

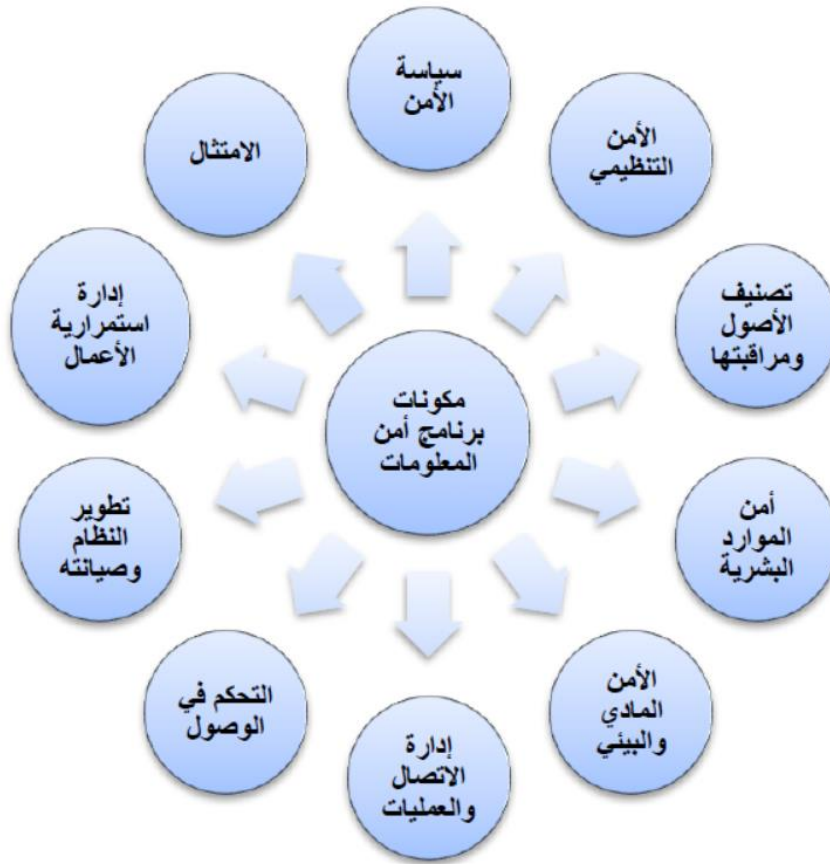
معظم المنظمات قد لا يكون لديها فهم واضح فيما يختص ببرنامج أمن المعلومات وأهدافه وكيفية بنائه، لذلك يجب النظر إلى أفضل الممارسات في هذه الصناعة للحصول على بعض التوجيه، فالمبدأ التوجيهي الأكثر استخداماً في جميع أنحاء العالم لبناء برامج الامن هو (ISO 27001:2005)، الذي تم اشتقاقه من المعيار البريطاني القياسي (BS 7799)، وهو معيار معترف به دولياً لإدارة أمن المعلومات يوفر توصيات مفاهيمية رفيعة المستوى بشأن أمن المنظمة، ويتألف هذا المعيار من جزئين هما:

- الجزء الأول: هو دليل تنفيذ مع مبادئ توجيهية حول كيفية بناء بنيته تحتية شاملة لأمن المعلومات.
- الجزء الثاني: هو دليل لمراجعة الحسابات يستند إلى المتطلبات التي يجب تلبيتها لكي تعتبر المنظمة متوافقة مع المعيار (ISO 27001:2005)، ويتم تقسيم المستند إلى المكونات التالية:
 ١. سياسة أمن المعلومات للمنظمة: وهي بمثابة خريطة لأهداف العمل ودعم الإدارة والأهداف والمسؤوليات الأمنية.
 ٢. الأمن التنظيمي: وهو إنشاء وصيانة هيكل أمني تنظيمي من خلال استخدام منتدى الأمن، وضابط الأمن وتحديد المسؤوليات الأمنية، وعملية الترخيص، والاستعانة بمصادر خارجية، والمراجعة المستقلة.
 ٣. تصنيف الأصول ومراقبتها: حيث تطوير بنية تحتية أمنية لحماية الأصول التنظيمية من خلال إجراءات المساءلة والجرد والتصنيف.
 ٤. أمن الموارد البشرية: وهو الحد من المخاطر الكامنة في التفاعل البشري من خلال فحص الموظفين، وتحديد الأدوار

والمسؤوليات، وتدريب الموظفين بشكل صحيح وتوثيق تداعيات عدم تلبية التوقعات.

٥. الأمن المادي والبيئي: وهو حماية أصول المنظمة عن طريق اختيار موقع المنظمة بشكل صحيح، وإقامة وصيانة المحيط الأمني، وتنفيذ مراقبة الدخول وحماية المعدات.

٦. التحكم في الوصول: حيث تم التحكم في الوصول إلى الأصول استناداً إلى متطلبات العمل وإدارة الهوية وأساليب المصادقة والمراقبة.



رسم توضيحي لمكونات برنامج أمن المعلومات ١

٧. إدارة الاتصالات والعمليات: وذلك من خلال تنفيذ أمن العمليات حيث الإجراءات التشغيلية، ومراقبة التغيير السليم، والتعامل مع الحوادث، والفصل بين الواجبات، وتخطيط القدرات وإدارة الشبكات، والتعامل مع وسائل الاعلام.

٨. تطوير النظام وصيانتة: حيث تنفيذ الأمن في جميع مراحل عمر النظام من خلال التطوير والتنفيذ والصيانة والتخلص.
٩. إدارة استمرارية الاعمال: مكافحة تعطيل العمليات العادية باستخدام تخطيط الاستمرارية والاختبار.
١٠. الامتثال: الامتثال للمتطلبات التنظيمية والتعاقدية والقانونية باستخدام الضوابط التقنية، ومراجعة حسابات النظام والوعي القانوني.

برنامج امن المعلومات (وزارة الموارد البشرية في المملكة):

تولي وزارة الموارد البشرية والتنمية الاجتماعية اهتمام كبير لرؤية المملكة العربية السعودية ٢٠٣٠. حيث أن أحد أهم مستهدفاتها هو التحول نحو العالم الرقمي لذلك فإن الهدف الرئيسي لإدارة أمن المعلومات هو خلق بيئة عمل آمنة للوزارة من خلال ضمان حماية الأصول المعلوماتية والحفاظ على سريتها وسلامتها وتوفيرها عند الحاجة

رؤية واهداف إدارة امن المعلومات:

- بناء استراتيجية متكاملة تشمل تقييم المخاطر وتحليلها والتأكد من أمان وسلامة كافة الأنظمة بشكل مستمر.
- تحقيق أعلى درجات الالتزام بضوابط للأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني لضمان تقليل المخاطر المتعلقة به على الأصول المعلوماتية والتقني.
- بناء وتطوير السياسات والإجراءات الخاصة بأمن معلومات التي سيلتزم بها كافة منسوبي الوزارة لضمان حماية الأصول المعلوماتية.

- مراقبة وحماية جميع شبكات وأنظمة الوازرة والكشف عن الهجمات الالكترونية ومحاولات الاختراق والتعامل السريع معها لمنع حدوثها أو الحد من آثارها.

- التوافق مع المعايير الدولية لأمن المعلومات (مثل ISO27001)؛ لتحقيق إدارة أصول معلومات آمنة وعالية الخصوصية، إلى جانب حمايتها.

- تقديم برامج توعوية تفاعلية تغطي كافة المواضيع الهامة في أمن المعلومات والمخاطر وتهديدات لرفع مستوى وعي كافة منسوبي الوزارة.

يعتبر أمن المعلومات أحد أهم العناصر التي تقوم عليها القطاعات المختلفة داخل الوزارة وذلك لارتباطها بشكل وثيق بتنفيذ الأعمال وتقديم الخدمات بشكل إلكتروني آمن يوفر السرعة والمرونة والدقة اللازمة وأيضا تحقيق مستوى الحماية المطلوبة للأصول المعلوماتية والبيانات في إطار بنية تحتية آمنة وفقاً لأفضل الممارسات والمعايير التقنية والأمنية والمتطلبات التشريعية والتنظيمية ذات العلاقة وتشمل:

- الضوابط والإرشادات الصادرة من الهيئة الوطنية للأمن السيبراني.

- نظام مكافحة جرائم المعلوماتية

- نظام التعاملات الإلكترونية.

- نظام الاتصالات.

- نظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها (البشرية، ٢٠٢٤).

- أهداف برامج أمن المعلومات:

توجد عدة أهداف رئيسية وفرعية لبرامج أمن المعلومات، ولكن تتمثل الأهداف الرئيسية في جميع برامج الأمن في:

- سرية المعلومات: وهي إخفاء المعلومات أو الموارد بمعنى حماية المعلومات من عدم اطلاع أي شخص غير مخول له بالاطلاع عليها.
- تكاملية المعلومات (سلامة المحتوى): تكاملية المعلومات تعني ضمان سلامة محتوى المعلومات وضمان عدم تغييرها أو تدميرها من قبل جهات غير مخولة.
- إتاحة المعلومات (القدرة على الوصول): وتعني التأكد من استمرار عمل نظام المعلومات، واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمستخدم المعلومات وتوافرها عند الحاجة إليها، والتأكد من أن مستخدمي تلك المعلومات لن يتعرضوا إلى منع استخدامهم لها بطريقة غير مشروعة.

الفصل الثالث

الإطار العملي للدراسة

مقدمة:

يهدف هذا الفصل إلى عرض نتائج استخدام بعض اساليب الإحصائية الوصفية التي افرزتها الاستبانة، من خلال تحليل اراء المبحوثين حول دور الأمن السيبراني في حماية الأنظمة المعلوماتية، حيث تم التوزيع التكراري والنسب المئوية والأوساط الحسابية لتقدير المستويات، والانحرافات المعيارية، وللإجابة عن اسئلة الدراسة سنستعين في إجابات المبحوثين الآتية:

أولاً: ترميز إجابات برنامج التحليل الاحصائي (SPSS)

ترميز إجابات الأسئلة الشخصية (النوع)

تم ترميز الاجابات للبيانات الشخصية (ذكر - انثى) في برنامج التحليل الاحصائي كالتالي:

ذكر	١
انثى	٢

جدول ١ البيانات الشخصية (النوع)

ترميز إجابات الأسئلة الشخصية (العمر)

تم ترميز الاجابات للبيانات الشخصية (العمر) في برنامج التحليل الاحصائي كالتالي:

أقل من ١٨ عاماً	١
من ١٨ - ٢٤ عاماً	٢
من ٢٥ - ٣٤ عاماً	٣

من ٣٥-٤٥ عاماً	٤
من ٤٦ فأكثر	٥

جدول ٢ البيانات الشخصية (العمر)

ترميز إجابات الأسئلة الشخصية (المستوى التعليمي)

تم ترميز الاجابات للبيانات الشخصية (المستوى التعليمي) في برنامج التحليل الاحصائي كالتالي:

ثانوي	١
دبلوم	٢
جامعي	٣
دراسات عليا	٤

جدول ٣ البيانات الشخصية (المستوى التعليمي)

ترميز إجابات أسئلة المحاور الثلاثة

تم ترميز الاجابات للأسئلة في برنامج التحليل الاحصائي كالتالي:

موافق جداً	١
موافق	٢
محايد	٣

غير موافق	٤
غير موافق جدا	٥

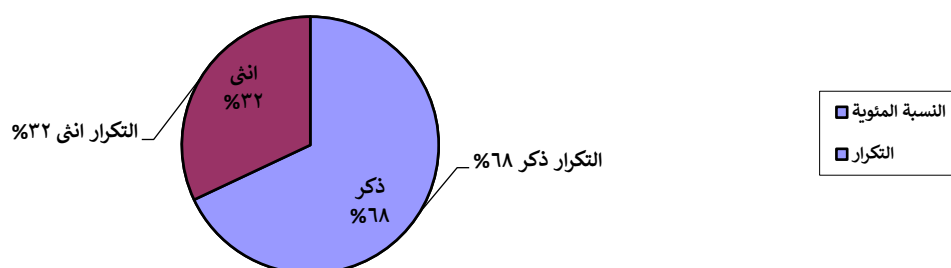
جدول ٤ : ترميز إجابات برنامج التحليل الإحصائي (SPSS)

ثانياً: نسبة تكرار الاسئلة الشخصية:

١- النوع

النسبة التراكمية	النسبة المئوية	التكرار	
٦٨	٦٨	٣٤	ذكر
١٠٠	٣٢	١٦	موافق
	١٠٠	٥٠	الاجمالي

جدول ٥ تكرار الاسئلة الشخصية (النوع)



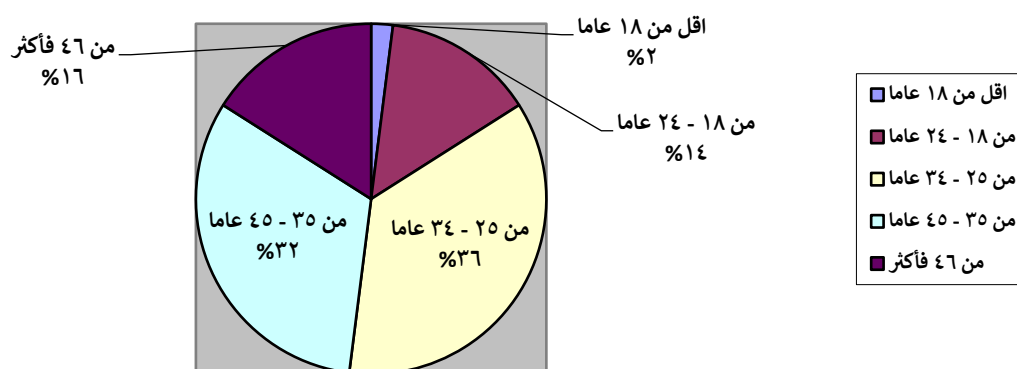
رسم توضيحي ٢ نسبة التكرار للأسئلة الشخصية (النوع)

بلغت نسبة التكرار للمعلومات الشخصية (النوع) حيث حازت الذكور على النسبة الاعلى بمعدل ٦٨٪ بعدد بلغ ٣٤ من نسبة المبحوثين وحازت الاناث على النسبة الاقل بمعدل ٣٢٪ بعدد بلغ ١٦ شخص من نسبة المبحوثين.

٢- العمر

النسبة التراكمية	النسبة المئوية	التكرار	
٢	٢	١	أقل من ١٨ عاما
١٦	١٤	٧	من ١٨ - ٢٤ عاما
٥٢	٣٦	١٨	من ٢٥ - ٣٤ عاما
٨٤	٣٢	١٦	من ٣٥ - ٤٥ عاما
١٠٠	١٦	٨	من ٤٦ فأكثر
	١٠٠	٧٢	الاجمالي

جدول ٦ تكرار الأسئلة الشخصية (العمر)



رسم توضيحي ٣ تكرار الأسئلة الشخصية (العمر)

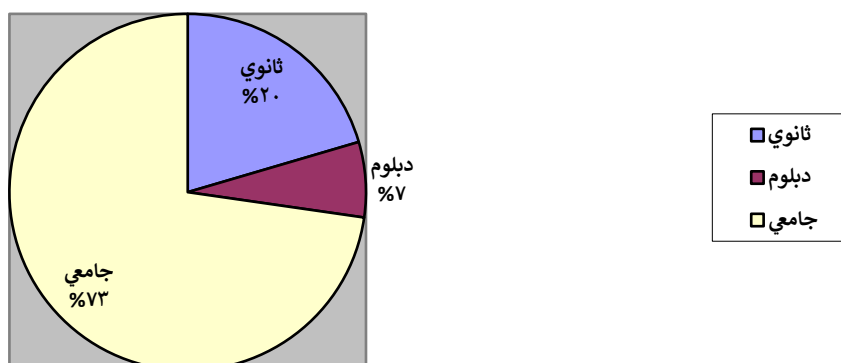
بلغت نسبة التكرار للمعلومات الشخصية (العمر) حيث حازت (٢٥ - ٣٤) على النسبة الاعلى بمعدل ٣٦% بعدد بلغ ١٨ شخص من نسبة المبحوثين وحازت (٣٥-٤٥) على ثاني نسبة بمعدل ٣٢% من نسبة المبحوثين بعدد

بلغ ١٦ شخص من نسبة المبحوثين، وحازت (٤٦ فأكثر) على ثالث نسبة بمعدل بلغ ١٦٪ من نسبة المبحوثين بعدد بلغ ٨ شخص من نسبة المبحوثين وحازت النسب (١٨-٢٤) و (اقل من ١٨) على النسب الاقل تالياً بمعدل ١٤٪ و ٢٪ بعدد ٧ و ١ من نسبة المبحوثين.

٣- المستوى التعليمي

النسبة التراكمية	النسبة المئوية	التكرار	
١٨	١٨	٩	ثانوي
٢٤	٦	٣	دبلوم
٨٨	٦٤	٣٢	جامعي
١٠٠	١٢	٦	دراسات عليا
	١٠٠	٥٠	الاجمالي

جدول ٧ تكرار الأسئلة الشخصية (المستوى التعليمي)



رسم توضيحي ٤ تكرار الأسئلة الشخصية (المستوى التعليمي)

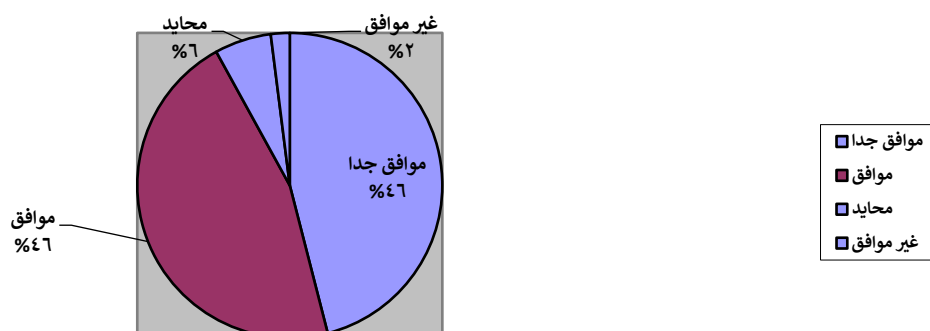
بلغت نسبة التكرار للمعلومات الشخصية (المستوى التعليمي) حيث حازت (جامعي) على النسبة الاعلى بمعدل ٦٤٪ بعدد بلغ ٣٢ شخص من نسبة المبحوثين وحازت (ثانوي) على ثاني نسبة بمعدل بلغ ١٨٪ من نسبة المبحوثين بعدد بلغ ٩ اشخاص من نسبة المبحوثين وحازت النسبة (دراسات عليا) و (دبلوم) توالياً على النسبة الاقل بمعدل بلغ ١٢٪ و ٦٪ من نسبة المبحوثين بعدد بلغ ٦ و ٣ اشخاص من نسبة المبحوثين

ثالثاً: نسبة تكرار أسئلة المحور الأول

السؤال الأول: يتم مراجعة وتطوير سياسة أمن المعلومات بشكل دوري

التكرار	النسبة المئوية	النسبة التراكمية
موافق جداً	٢٣	٤٦
موافق	٢٣	٩٢
محايد	٣	٩٨
غير موافق	١	١٠٠
الاجمالي	٥٠	١٠٠

جدول ٨ نسبة تكرار أسئلة المحور الأول السؤال الأول



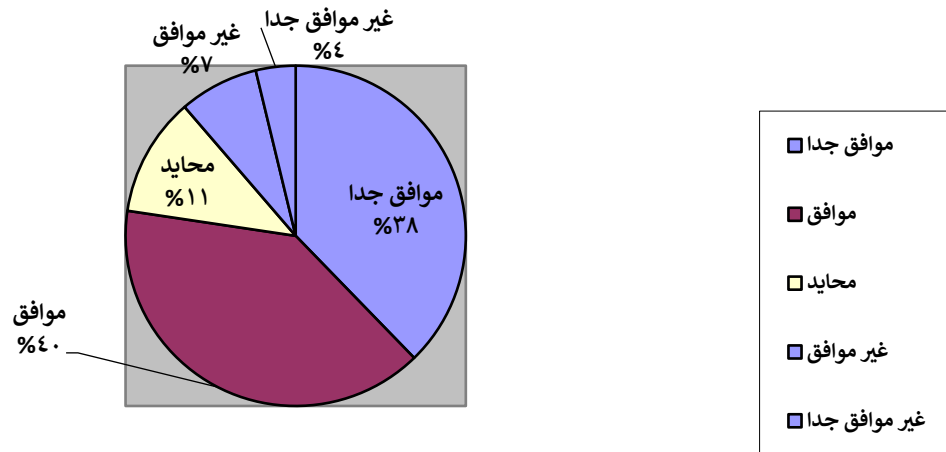
رسم توضيحي ٥ نسبة تكرار أسئلة المحور الأول للسؤال الأول

بلغت نسبة اجابات المبحوثين للسؤال الاول حيث حازت إجابات المبحوثين على فقرة (موافق جدا) و (موافق) على النسبة الاعلى بمعدل ٤٦٪ لكل منهما بعدد بلغ ٢٣ لكل منهما من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٦٪ بعدد بلغ ٣ اشخاص من نسبة المبحوثين، وهذا يدل على إجماع كامل على موافقة المبحوثين على انه يتم مراجعة وتطوير سياسة أمن المعلومات بشكل دوري بنسبة موافقة بلغت ١٠٠٪.

السؤال الثاني: يتم إدخال المعلومات والبيانات بعد المصادقة من المدير المباشر

التكرار	النسبة المئوية	النسبة التراكمية	
٢٠	٤٠	٤٠	موافق جدا
٢١	٤٢	٨٢	موافق
٦	١٢	٩٤	محايد
٢	٤	٩٨	غير موافق
١	٢	١٠٠	غير موافق جدا
٥٠	١٠٠		الاجمالي

جدول ٩ نسبة تكرار أسئلة المحور الأول السؤال الثاني



رسم توضيحي ٦ نسبة تكرار أسئلة المحور الأول السؤال الثاني

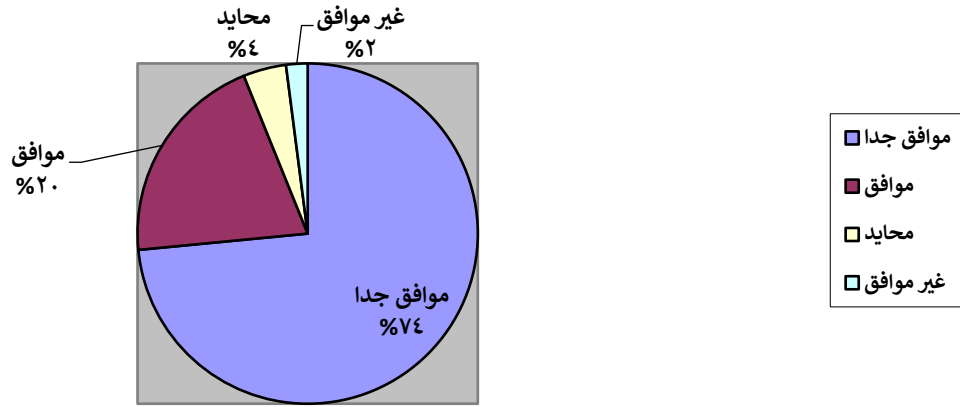
بلغت نسبة اجابات المبحوثين للسؤال الثاني حيث حازت إجابات المبحوثين على فقرة (موافق) على النسبة الاعلى بمعدل ٤٢٪ بعدد بلغ ٢١ من نسبة المبحوثين وحازت الاجابة (موافق جدا) على النسبة الثانية بمعدل ٤٠٪ بعدد بلغ ٢٠ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ١٢٪ بعدد بلغ ٦ ، وبلغت النسبة الأخيرة (غير موافق) و (غير موافق جدا) تواليا على نسبة ٤٪ و ٢٪ بعدد بلغ ٤ و ٢ تواليا وهذا يدل على إجماع كامل على موافقة المبحوثين على أنه يتم إدخال المعلومات والبيانات بعد المصادقة من المدير المباشر بنسبة موافقة كبيرة بلغت ٨٢٪ من إجابات المبحوثين.

السؤال الثالث: لا يسمح لغير المختصين بالوصول إلى أجهزة الحاسب والعتاد المحوسب

المرادف	التكرار	النسبة المئوية	النسبة التراكمية
موافق جدا	٣٦	٧٢	٧٢
موافق	١٠	٢٠	٩٢
محايد	٢	٤	٩٦

غير موافق	١	٢	٩٨
غير موافق جدا	١	٢	١٠٠
الاجمالي	٥٠	١٠٠	

جدول ١٠ نسبة تكرار أسئلة المحور الأول السؤال الثالث



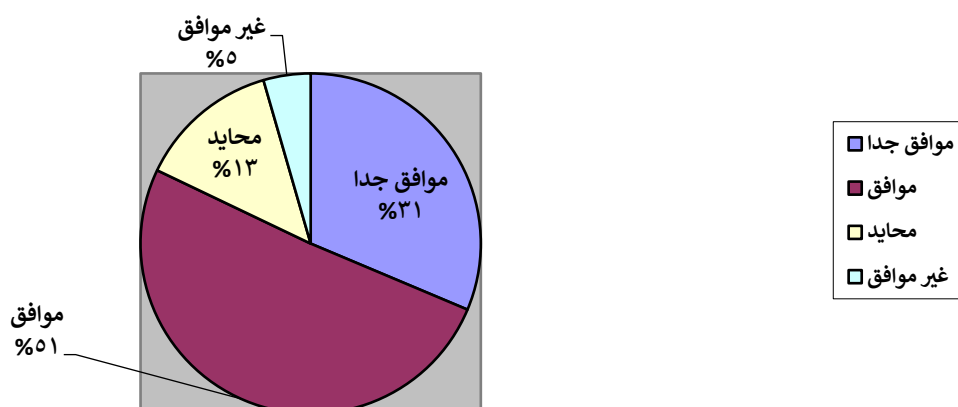
رسم توضيحي ٧ نسبة تكرار أسئلة المحور الأول السؤال الثالث

بلغت نسبة اجابات المبحوثين للسؤال الثالث على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٧٢٪ بعدد بلغ ٣٦ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٠٪ بعدد بلغ ١٠ اشخاص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ٤٪ بعدد بلغ ٢، وحازت كلا من الاجابة (غير موافق) و (غير موافق جداً) على اجابة واحدة فقط بنسبة بلغت ٢٪ بعدد بلغ ١ لكل منهما وهذا يدل على إجماع كامل على موافقة المبحوثين على أنه لا يسمح لغير المختصين بالوصول إلى أجهزة الحاسب الالى والعتاد المحوسب بنسبة موافقة كبيرة بلغت ٩٢٪ من إجابات المبحوثين.

السؤال الرابع: يمنع الدخول لمواقع الانترنت بالأجهزة الموصول بالخادم المركزي

التكرار	النسبة المئوية	النسبة التراكمية	
٢١	٤٢	٤٢	موافق جدا
١٧	٣٤	٧٣	موافق
٩	١٨	٩٤	محايد
٣	٦	١٠٠	غير موافق
٥٠	١٠٠		الاجمالي

جدول ١١ نسبة تكرار أسئلة المحور الأول السؤال الرابع



رسم توضيحي ٨ نسبة تكرار أسئلة المحور الأول السؤال الرابع

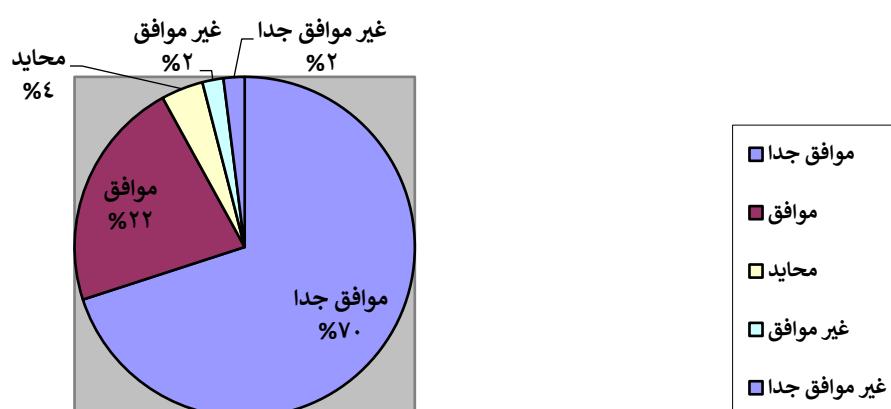
بلغت نسبة اجابات المبحوثين للسؤال الرابع على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٤٢٪ بعدد بلغ ٢١ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٣٤٪ بعدد بلغ ١٧ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ١٨٪ بعدد بلغ ٩، وحازت الاجابة (غير موافق) على ثلاث إجابات فقط

بنسبة بلغت ٦٪ وهذا يدل على إجماع كامل على موافقة المبحوثين على أنه يمنع الدخول لمواقع الانترنت بالأجهزة الموصول بالخادم المركزي بنسبة موافقة كبيرة بلغت ٧٦٪ من إجابات المبحوثين.

السؤال الخامس: لا يسمح بتنشيط البرامج غير المرخصة والمقرصنة

التكرار	النسبة المئوية	النسبة التراكمية	
٣٥	٧٠	٧٠	موافق جدا
١١	٢٢	٩٢	موافق
٢	٤	٩٦	محايد
١	٢	٩٨	غير موافق
١	٢	١٠٠	غير موافق جدا
٥٠	١٠٠		الاجمالي

جدول ١٢ نسبة تكرار أسئلة المحور الأول السؤال الخامس



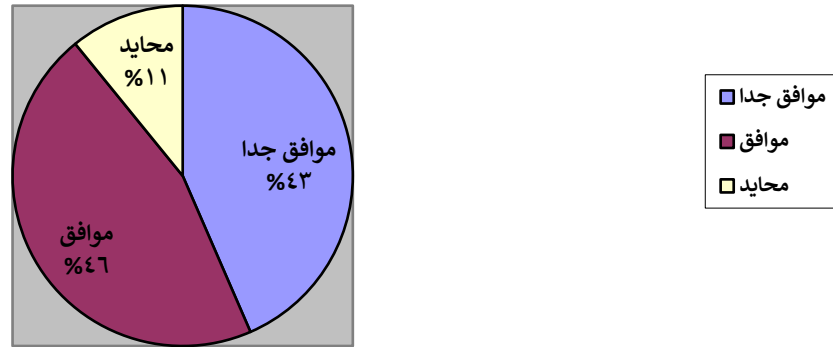
رسم توضيحي ٩ نسبة تكرار أسئلة المحور الأول السؤال الخامس

بلغت نسبة اجابات المبحوثين للسؤال الخامس على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٧٠٪ بعدد بلغ ٣٥ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٢٪ بعدد بلغ ١١ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ٤٪ بعدد بلغ ٢، وحازت الاجابة (غير موافق) و (غير موافق جدا) على اجابة واحد فقط بنسبة بلغت ٢٪ لعدد ١، وهذا يدل على إجماع كامل على موافقة المبحوثين على انه لا يسمح بتثبيت البرامج غير المرخصة والمقرصنة بنسبة موافقة كبيرة بلغت ٩٢٪ من إجابات المبحوثين.

السؤال السادس: يتم التصريح بعناوين الحواسيب Ip حتى يتم دخول النظام

النسبة التراكمية	النسبة المئوية	التكرار	
٤٠	٤٠	٢٠	موافق جدا
٨٢	٤٢	٢١	موافق
٩٢	١٠	٥	محايد
١٠٠	٨	٤	غير موافق
	١٠٠	٥٠	الاجمالي

جدول ١٣ نسبة تكرار أسئلة المحور الأول السؤال السادس



رسم توضيحي ١٠ نسبة تكرار أسئلة المحور الأول السؤال السادس

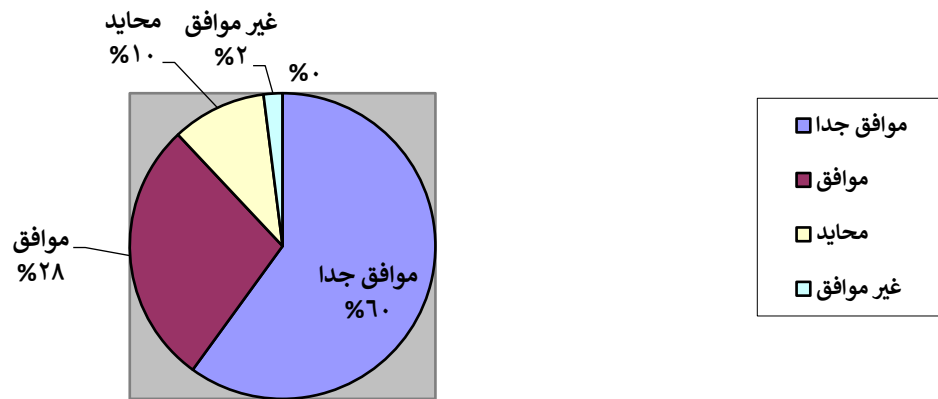
بلغت نسبة اجابات المبحوثين للسؤال السادس على فقرة (موافق) على النسبة الاعلى بمعدل ٤٢٪ بعدد بلغ ٢١ من نسبة المبحوثين وحازت الاجابة (موافق جداً) على النسبة الثانية بمعدل ٤٠٪ بعدد بلغ ٢٠ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) و (غير موافق) توالياً على ٥ و ٤ إجابات بنسبة بلغت ١٠٪ و ٨٪ توالياً، وهذا يدل على إجماع كامل على أنه يتم التصريح بعناوين الحواسيب Ip حتى يتم دخول النظام، بنسبة موافقة كبيرة بلغت ٨٢٪ من إجابات المبحوثين.

السؤال السابع: تسجيل أي عملية أثناء المعالجة باسم الموظف الذي قام بها مع التوقيت

النسبة التراكمية	النسبة المئوية	التكرار	
٦٠	٦٠	٣٠	موافق جداً
٨٨	٢٨	١٤	موافق
٩٨	١٠	٥	محايد
١٠٠	٢	١	غير موافق

الاجمالي	٥٠	١٠٠	
----------	----	-----	--

جدول ١٤ نسبة تكرار أسئلة المحور الأول السؤال السابع



رسم توضيحي ١١ نسبة تكرار أسئلة المحور الأول السؤال السابع

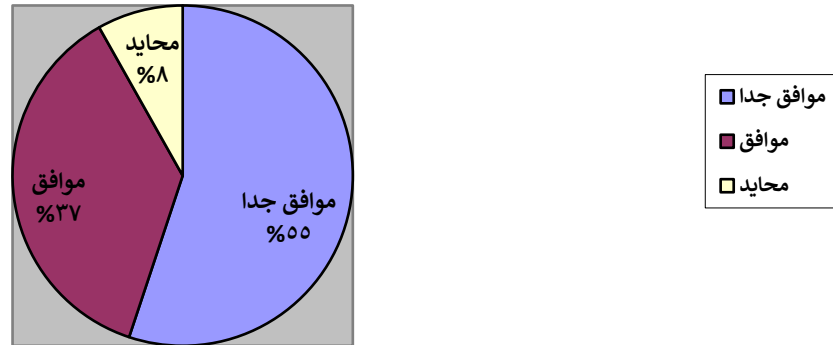
بلغت نسبة اجابات المبحوثين للسؤال السابع على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٠٪ بعدد بلغ ٣٠ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٨٪ بعدد بلغ ١٤ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ١٠٪ بعدد بلغ ٥، وحازت الاجابة (غير موافق) على النسبة الأخيرة بإجابة واحدة فقط بنسبة بلغت ٢٪، وهذا يدل على إجماع على أنه يتم تسجيل أي عملية أثناء المعالجة باسم الموظف الذي قام بها مع التوقيت بنسبة موافقة عالية بلغت ٨٨٪ من إجابات المبحوثين.

رابعاً: نسبة تكرار أسئلة المحور الثاني

السؤال الأول: يتم تدريب العاملين على نظم المحوسبة بشكل دوري لتطوير مهاراتهم المتعلقة بالمستجدات الامنية

التكرار	النسبة المئوية	النسبة التراكمية	
٢٧	٥٤	٥٤	موافق جداً
١٨	٣٦	٩٠	موافق
٤	٨	٩٨	محايد
١	٢	١٠٠	غير موافق
٥٠	١٠٠		الاجمالي

جدول ١٥ نسبة تكرار أسئلة المحور الثاني السؤال الأول



رسم توضيحي ١٢ نسبة تكرار أسئلة المحور الثاني السؤال الأول

بلغت نسبة اجابات المبحوثين للسؤال الأول على فقرة (موافق جداً) على النسبة الاعلى بمعدل ٥٤٪ بعدد بلغ ٢٧ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٣٦٪ بعدد بلغ ١٨ شخص من

نسبة المبحوثين، وحازت الإجابة (محايد على الإجابة الثالثة بنسبة بلغت ٨٪ وعدد ٤، وحازت الإجابة (محايد) على إجابة واحدة فقط بنسبة بلغت ٤,١٪ وهذا يدل على إجماع كامل على أنه يتم تدريب العاملين على نظم المحوسبة بشكل دوري لتطوير مهاراتهم المتعلقة بالمستجدات الأمنية بنسبة موافقة كبيرة بلغت ٩٠٪ من إجابات المبحوثين.

السؤال الثاني: يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص المؤسسة كجزء من شروط التوظيف

التكرار	النسبة المئوية	النسبة التراكمية	
٣٤	٦٨	٦٨	موافق جدا
١٢	٢٤	٩٢	موافق
١	٢	٩٤	محايد
٣	٦	١٠٠	غير موافق
٥٠	١٠٠		الاجمالي

جدول ١٦ نسبة تكرار أسئلة المحور الثاني السؤال الثاني



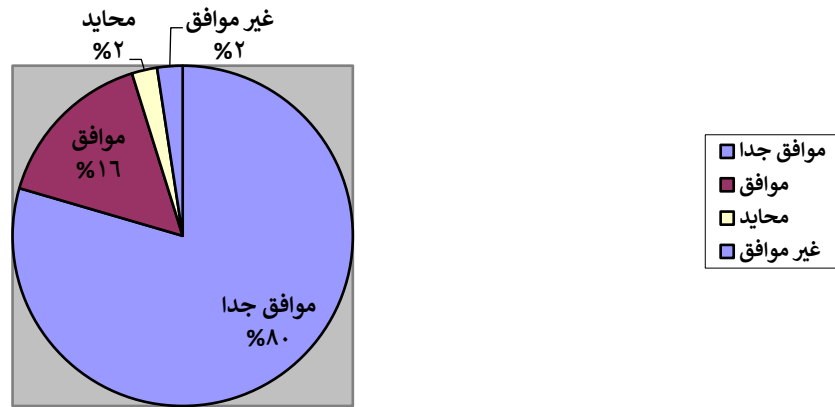
رسم توضيحي ١٣ نسبة تكرار أسئلة المحور الثاني السؤال الثاني

بلغت نسبة اجابات المبحوثين للسؤال الثاني على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٨٪ بعدد بلغ ٣٤ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٤٪ بعدد بلغ ١٢ شخص من نسبة المبحوثين، وحازت الاجابة (غير موافق) على النسبة الثالثة بمعدل بلغ ٦٪ بعدد بلغ ٣، وحازت الاجابة (محايد) على اجابة واحدة فقط بنسبة بلغت ٢٪ وهذا يدل على إجماع كامل على موافقة المبحوثين على أنه يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص المؤسسة كجزء من شروط التوظيف بنسبة موافقة كبيرة بلغت ٩٢٪ من إجابات المبحوثين.

السؤال الثالث: يطلب من الموظف والمتعاقدين الإبلاغ عن أي نقاط ضعف يلاحظونها في الانظمة

النسبة التراكمية	النسبة المئوية	التكرار	
٦٦	٦٦	٣٣	موافق جدا
٩٢	٢٦	١٣	موافق
٩٦	٤	٢	محايد
١٠٠	٤	٢	غير موافق
	١٠٠	٥٠	الاجمالي

جدول ١٧ نسبة تكرار أسئلة المحور الثاني السؤال الثالث



رسم توضيحي ١٤ نسبة تكرار أسئلة المحور الثاني السؤال الثالث

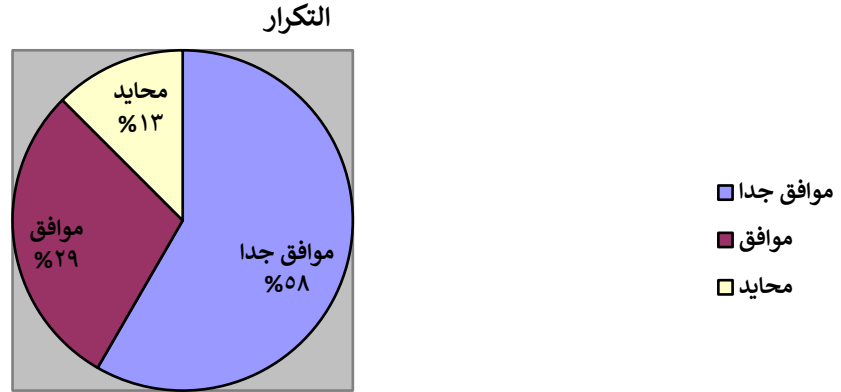
بلغت نسبة اجابات المبحوثين للسؤال الثالث على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٦٪ بعدد بلغ ٣٣ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٦٪ بعدد بلغ ١٣ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) و (غير موافق) على إجابتين فقط بنسبة بلغت ٢,٨٪ وهذا يدل على إجماع كامل على موافقة المبحوثين على ان يطلب من الموظفين والمتعاقدين الإبلاغ عن أي نقاط ضعف يلاحظونها في الانظمة بنسبة موافقة كبيرة بلغت ٩٦٪ من إجابات المبحوثين.

السؤال الرابع: هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث امن المعلومات

التكرار	النسبة المئوية	النسبة التراكمية	
موافق جدا	٢٨	٥٦	٥٦
موافق	١٤	٢٨	٨٤
محايد	٦	١٢	٩٦
غير موافق	١	٢	٩٨

غير موافق جدا	١	٢	١٠٠
الاجمالي	٥٠	١٠٠	

جدول ١٨ نسبة تكرار أسئلة المحور الثاني السؤال الرابع



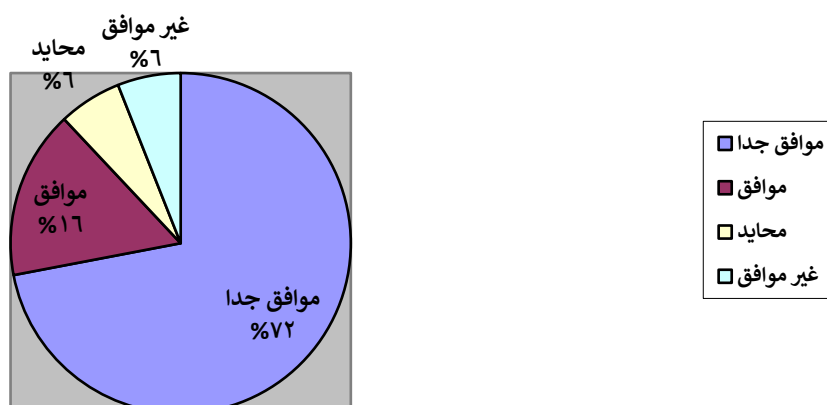
رسم توضيحي ١٥ نسبة تكرار أسئلة المحور الثاني السؤال الرابع

بلغت نسبة اجابات المبحوثين للسؤال الرابع على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٧٠,٨٪ بعدد بلغ ٥١ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٦,٤٪ بعدد بلغ ١٩ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على إجابتين فقط بنسبة بلغت ٢,٨٪ وهذا يدل على إجماع كامل على موافقة المبحوثين على ان يسارع المستخدمون للاستفادة من العروض التي يتم تقديمها بنسبة موافقة كبيرة بلغت ٩٧,٢٪ من إجابات المبحوثين.

السؤال الخامس: يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة

التكرار	النسبة المئوية	النسبة التراكمية	
٣٦	٧٢	٧٢	موافق جدا
٨	١٦	٨٨	موافق
٣	٦	٩٤	محايد
٣	٦	١٠٠	غير موافق
٥٠	١٠٠		الاجمالي

جدول ١٩ نسبة تكرار أسئلة المحور الثاني السؤال الخامس



رسم توضيحي ١٦ نسبة تكرار أسئلة المحور الثاني السؤال الخامس

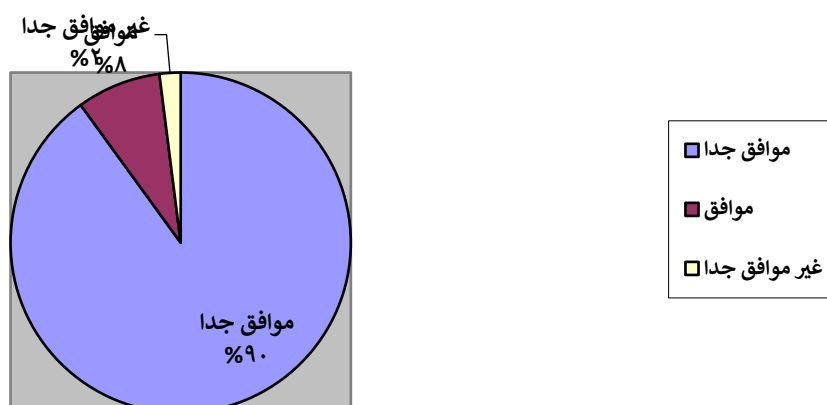
بلغت نسبة اجابات المبحوثين للسؤال الخامس على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٧٢٪ بعدد بلغ ٣٦ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ١٦٪ بعدد بلغ ٨ شخص من

نسبة المبحوثين، وحازت الاجابة (محايد) و (غير موافق) على النسبة الثالثة بمعدل بلغ ٦٪ بعدد بلغ ٦ لكل منهما، وهذا يدل على إجماع كامل على موافقة المبحوثين على انه يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة بنسبة موافقة كبيرة بلغت ٨٨٪ من إجابات المبحوثين.

السؤال السادس: لكل موظف كلمة السر الخاصة به

النسبة التراكمية	النسبة المئوية	التكرار	
٩٠	٩٠	٤٥	موافق جدا
٩٨	٨	٤	موافق
١٠٠	٢	١	غير موافق جدا
	١٠٠	٥٠	الاجمالي

جدول ٢٠ نسبة تكرار أسئلة المحور الثاني السؤال السادس



رسم توضيحي ١٧ نسبة تكرار أسئلة المحور الثاني السؤال السادس

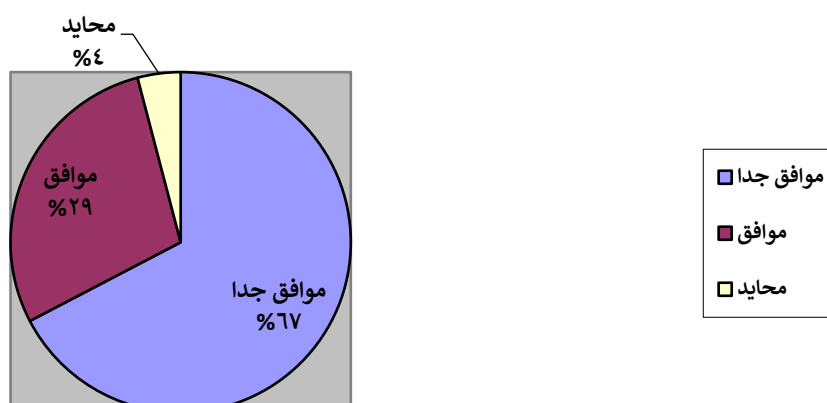
بلغت نسبة اجابات المبحوثين للسؤال السادس على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٩٠٪ بعدد بلغ ٤٥ من نسبة المبحوثين وحازت

الاجابة (موافق) على النسبة الثانية بمعدل ٨٪ بعدد بلغ ٤ شخص من نسبة المبحوثين، وحازت الاجابة (غير موافق جدا) على اجابه واحده فقط بنسبة بلغت ٢٪ وهذا يدل على إجماع كامل على موافقة المبحوثين على انه لكل موظف كلمة سر خاصة به بنسبة موافقة كبيرة بلغت ٩٨٪ من إجابات المبحوثين.

السؤال السابع: يطلب تغيير كلمة السر الخاصة بالموظف دورياً

النسبة التراكمية	النسبة المئوية	التكرار	
٦٦	٦٦	٣٣	موافق جدا
٩٤	٢٨	١٤	موافق
٩٨	٤	٢	محايد
١٠٠	٢	١	غير موافق جدا
	١٠٠	٥٠	الاجمالي

جدول ٢١ نسبة تكرار أسئلة المحور الثاني السؤال السابع



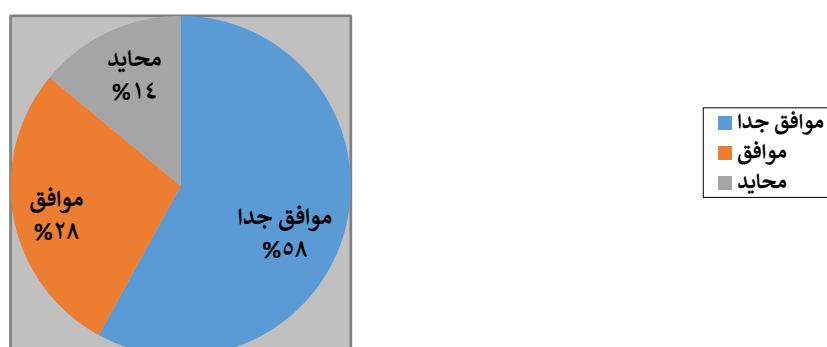
رسم توضيحي ١٨ نسبة تكرار أسئلة المحور الثاني السؤال السابع

بلغت نسبة اجابات المبحوثين للسؤال السابع على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٦٪ بعدد بلغ ٣٣ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٨٪ بعدد بلغ ١٤ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على إجابتين فقط بنسبة بلغت ٤٪، وبلغت الإجابة الأخيرة (غير موافق جدا) على إجابة واحدة فقط بنسبة ٢٪، وهذا يدل على إجماع كامل على أنه يتم تغيير كلمة المرور الخاصة بالموظف دورياً، بنسبة موافقة كبيرة بلغت ٩٤٪ من إجابات المبحوثين.

السؤال الثامن: توجد مراجعة دورية لصلاحيات المستخدمين للوصول إلى الأنظمة

التكرار	النسبة المئوية	النسبة التراكمية
موافق جدا	٢٩	٥٨
موافق	١٤	٨٦
محايد	٧	١٠٠
الاجمالي	٥٠	١٠٠

جدول ٢٢ نسبة تكرار أسئلة المحور الثاني السؤال الثامن



رسم توضيحي ١٩ نسبة تكرار أسئلة المحور الثاني السؤال الثامن

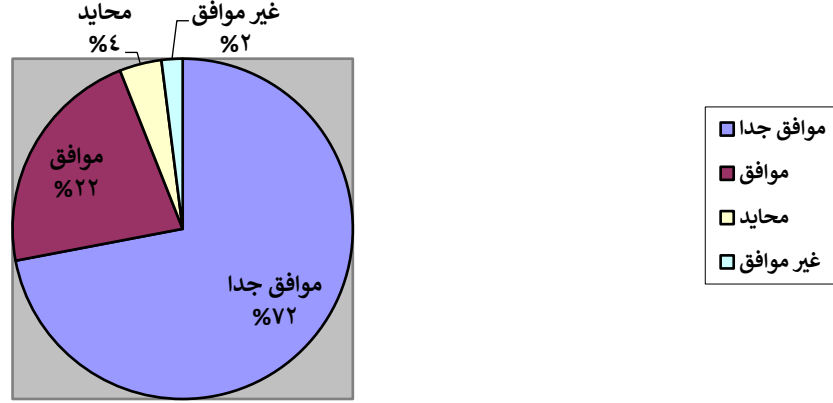
بلغت نسبة اجابات المبحوثين للسؤال الثامن على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٥٨٪ بعدد بلغ ٢٩ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٨٪ بعدد بلغ ١٤ شخص من نسبة المبحوثين، وحصلت الإجابة (محايد) على نسبة ١٤٪ من المبحوثين بعدد بلغ ١٤، وهذا يدل على إجماع كامل على أنه توجد مراجعة دورية لصلاحيات المستخدمة للوصول إلى الأنظمة، بنسبة موافقة كبيرة بلغت ٨٦٪ من إجابات المبحوثين.

خامسا: إجابات المحور الثالث

السؤال الأول: تستخدم المؤسسة شتى الوسائل (أبواب - أقفال - بطاقات دخول - كاميرات) لحماية مكونات الأنظمة المعلوماتية.

	التكرار	النسبة المئوية	النسبة التراكمية
موافق جدا	٣٦	٧٢	٧٢
موافق	١١	٢٢	٩٤
محايد	٢	٤	٩٨
غير موافق	١	٢	١٠٠
الاجمالي	٥٠	١٠٠	

جدول ٢٣ نسبة تكرار أسئلة المحور الثالث السؤال الأول



رسم توضيحي ١٩ نسبة تكرار أسئلة المحور الثالث السؤال الاول

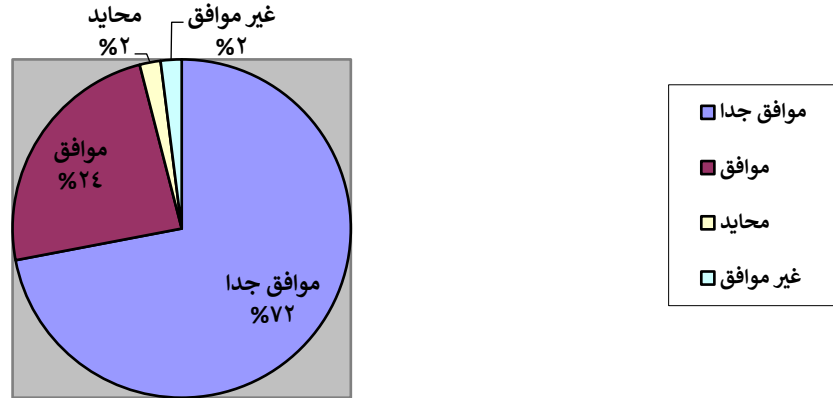
بلغت نسبة اجابات المبحوثين للسؤال الأول على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٧٢٪ بعدد بلغ ٣٦ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٢٪ بعدد بلغ ١١ شخص من نسبة المبحوثين، وحازت الاجابة (محايد - غير موافق) على اجابة واجابتين تواليا فقط بنسبة بلغت ٤٪ و ٢٪ لكل منهما، وهذا يدل على إجماع كامل على موافقة المبحوثين على انه تستخدم المؤسسة شتى الوسائل (أبواب - اقفال - بطاقات دخول - كاميرات) لحماية مكونات الأنظمة المعلوماتية بنسبة موافقة كبيرة بلغت ٩٤٪ من إجابات المبحوثين.

السؤال الثاني: يوجد في المؤسسة مصدر بديل للكهرباء إذا تم انقطاعها

النسبة التراكمية	النسبة المئوية	التكرار	
٧٢	٧٢	٣٦	موافق جدا

موافق	١٢	٢٤	٩٦
محايد	١	٢	٩٨
غير موافق	١	٢	١٠٠
الاجمالي	٥٠	١٠٠	

جدول ٢٤ نسبة تكرار أسئلة المحور الثالث السؤال الثاني



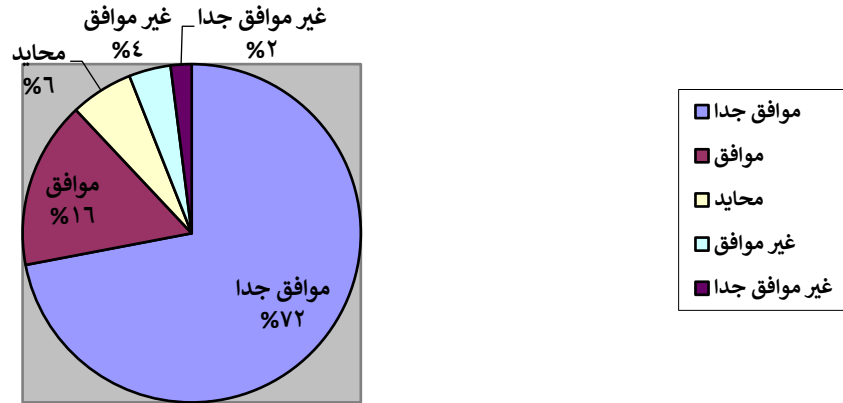
رسم توضيحي ٢٠ نسبة تكرار أسئلة المحور الثالث السؤال الثاني

بلغت نسبة اجابات المبحوثين للسؤال الثاني على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٧٢٪ بعدد بلغ ٣٦ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٤٪ بعدد بلغ ١٢ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) و (غير موافق) على النسبة الثالثة بمعدل بلغ ٢٪ بعدد بلغ ١ لكل منهما، وهذا يدل على إجماع على انه يوجد في المؤسسة مصدر بديل للكهرباء إذا تم انقطاعها بنسبة موافقة بلغت ٩٦٪ من إجابات المبحوثين.

السؤال الثالث: يمنع الموظف الغير مختص من اجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات

التكرار	النسبة المئوية	النسبة التراكمية	
٣٦	٧٢	٧٢	موافق جدا
٨	١٦	٨٨	موافق
٣	٦	٩٤	محايد
٢	٤	٩٨	غير موافق
١	٢	١٠٠	غير موافق جدا
٥٠	١٠٠		الاجمالي

جدول ٢٥ نسبة تكرار أسئلة المحور الثالث السؤال الثالث



رسم توضيحي ٢١ نسبة تكرار أسئلة المحور الثالث السؤال الثالث

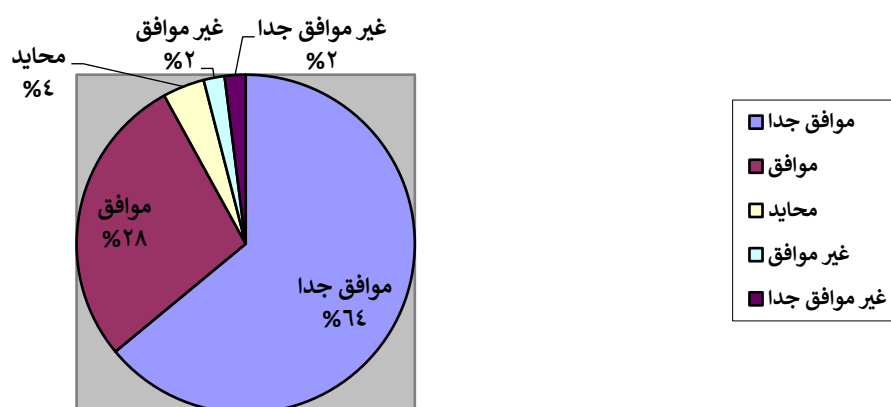
بلغت نسبة اجابات المبحوثين للسؤال الثالث على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٧٢٪ بعدد بلغ ٣٦ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ١٦٪ بعدد بلغ ٨ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ٦٪ بعدد بلغ ٣، وحازت الاجابة (غير موافق جدا - غير موافق) على (٢ -

١) تواليا بنسبة بلغت ٤٪ و ٢٪ وهذا يدل على إجماع كامل على موافقة المبحوثين على انه يمنع الموظف الغير مختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات بنسبة موافقة عالية بلغت ٨٨٪ من إجابات المبحوثين.

السؤال الرابع: كوابل الكهرباء والاتصالات التي تنقل البيانات او التي تدعم خدمات الأنظمة المعلوماتية محمية من العبث بها أو اتلافها.

التكرار	النسبة المئوية	النسبة التراكمية	
٣٢	٦٤	٦٤	موافق جدا
١٤	٢٨	٩٢	موافق
٢	٤	٩٦	محايد
١	٢	٩٨	غير موافق
١	٢	١٠٠	غير موافق جدا
٥٠	١٠٠		الاجمالي

جدول ٢٦ نسبة تكرار أسئلة المحور الثالث السؤال الرابع



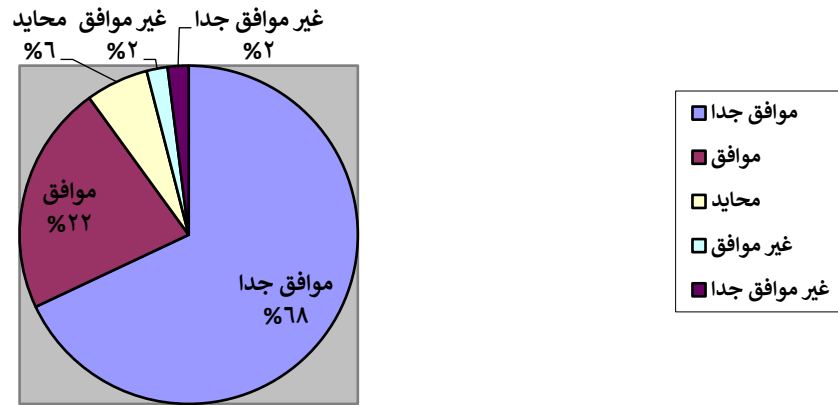
رسم توضيحي ٢٢ نسبة تكرار أسئلة المحور الثالث السؤال الرابع

بلغت نسبة اجابات المبحوثين للسؤال الرابع على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٤٪ بعدد بلغ ٣٢ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٨٪ بعدد بلغ ١٤ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ٤٪ بعدد بلغ ٢، وحازت الاجابة (غير موافق جدا - غير موافق) على (١) اجابات بنسبة بلغت ٢٪، وهذا يدل على إجماع عالي على موافقة المبحوثين أنه كوابل الكهرباء والاتصالات التي تنقل البيانات او التي تدعم خدمات الأنظمة المعلوماتية محمية من العبث بها أو اتلافها بنسبة موافقة كبيرة بلغت ٩٢٪ من إجابات المبحوثين.

السؤال الخامس: تستخدم طرق تشفير حماية البيانات

النسبة التراكمية	النسبة المئوية	التكرار	
٦٨	٦٨	٣٤	موافق جدا
٩٠	٢٢	١١	موافق
٩٦	٦	٣	محايد
٩٨	٢	١	غير موافق
١٠٠	٢	١	غير موافق جدا
	١٠٠	٥٠	الاجمالي

جدول ٢٧ نسبة تكرار أسئلة المحور الثالث السؤال الخامس



رسم توضيحي ٢٣ نسبة تكرار أسئلة المحور الثالث السؤال الخامس

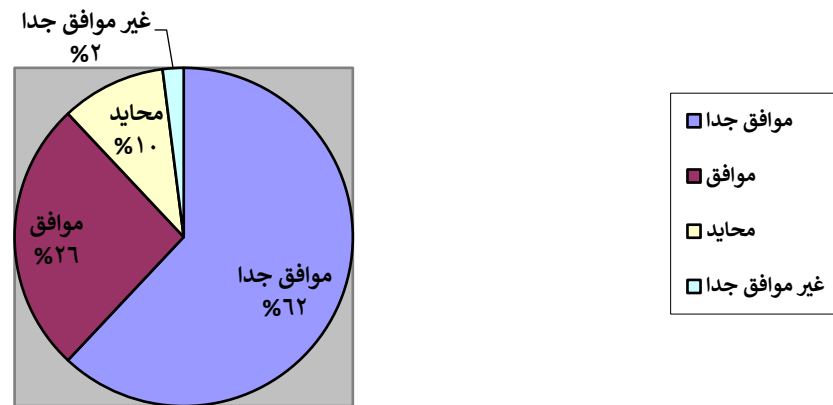
بلغت نسبة اجابات المبحوثين للسؤال الخامس على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٨٪ بعدد بلغ ٣٤ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٢٪ بعدد بلغ ١١ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ٦٪ بعدد بلغ ٣، وحازت الاجابة (غير موافق) و (غير موافق جدا) على اجابة واحده بنسبة بلغت ٢٪، وهذا يدل على إجماع كامل على أنه تستخدم طرق تشفير لحماية البيانات بنسبة موافقة كبيرة بلغت ٩٠٪ من إجابات المبحوثين.

السؤال السادس: توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات وفي مكان آمن

النسبة التراكمية	النسبة المئوية	التكرار	
٦٢	٦٢	٣١	موافق جدا
٨٨	٢٦	١٣	موافق

محايد	٥	١٠	٩٨
غير موافق جدا	١	٢	١٠٠
الاجمالي	٥٠	١٠٠	

جدول ٢٨ نسبة تكرار أسئلة المحور الثالث السؤال السادس



رسم توضيحي ٢٤ نسبة تكرار أسئلة المحور الثالث السؤال السادس

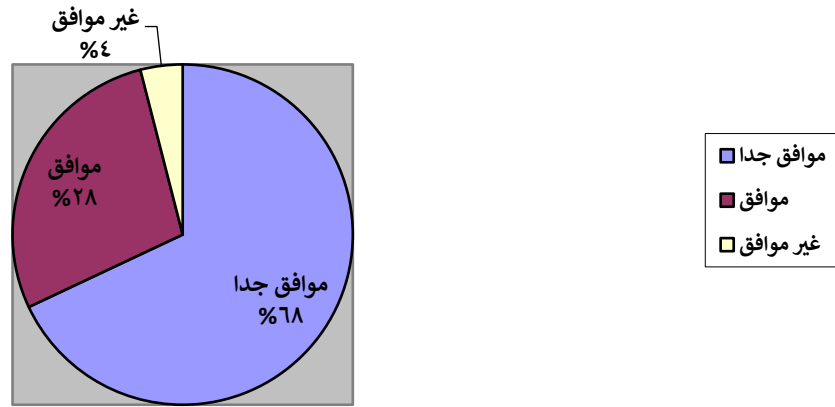
بلغت نسبة اجابات المبحوثين للسؤال السادس على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٢٪ بعدد بلغ ٣١ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ١٣٪ بعدد بلغ ٢٦ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ١٠٪ بعدد بلغ ٥، وحازت الاجابة (غير موافق جدا) على اجابة واحدة فقط بنسبة بلغت ٢٪ وهذا يدل على إجماع كامل على موافقة المبحوثين على توفر الأنظمة المستخدمة على خدمة النسخ الاحتياطي للبيانات وفي مكان آمن بنسبة موافقة كبيرة بلغت ٧٠,٨٪ من إجابات المبحوثين.

السؤال السابع: توجد برامج حماية لتتبع ومنع الاختراق والتسلل

التكرار	النسبة المئوية	النسبة التراكمية

موافق جدا	٣٤	٦٨	٦٨
موافق	١٤	٢٨	٩٦
غير موافق	٢	٤	١٠٠
الاجمالي	٥٠	١٠٠	

جدول ٢٩ نسبة تكرار أسئلة المحور الثالث السؤال السابع



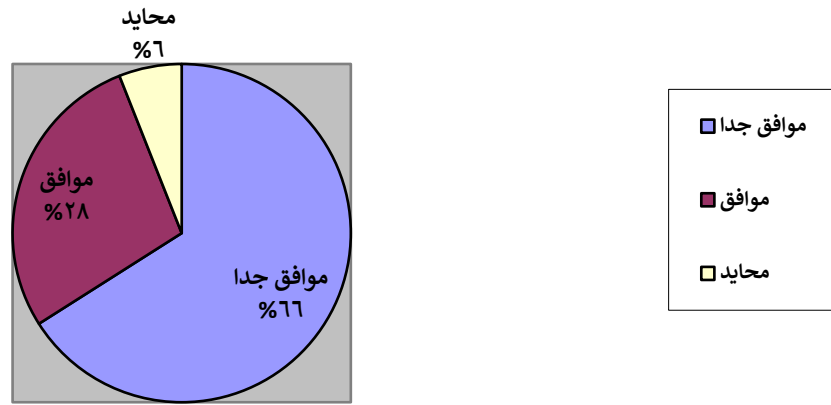
رسم توضيحي ٢٥ نسبة تكرار أسئلة المحور الثالث السؤال السابع

بلغت نسبة اجابات المبحوثين للسؤال السابع على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٨٪ بعدد بلغ ٣٤ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٨٪ بعدد بلغ ١٤ شخص من نسبة المبحوثين، وحازت الاجابة (غير موافق) على اجابتين فقط بنسبة بلغت ٤٪ وهذا يدل على إجماع كامل على موافقة المبحوثين على أنه توجد برامج حماية لتتبع ومنع الاختراق والتسلل بنسبة موافقة كبيرة بلغت ٩٦٪ من إجابات المبحوثين.

السؤال الثامن: تحتوي الشبكة على جدار ناري يحمي الشبكة من الاختراق

التكرار	النسبة المئوية	النسبة التراكمية	
٣٣	٦٦	٦٦	موافق جدا
١٤	٢٨	٩٤	موافق
٣	٦	١٠٠	محايد
٥٠	١٠٠		الاجمالي

جدول ٣٠ نسبة تكرار أسئلة المحور الثالث السؤال الثامن



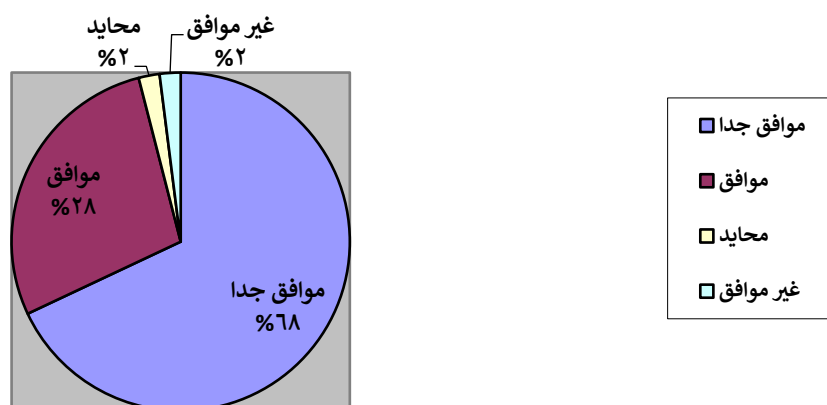
رسم توضيحي ٢٦ نسبة تكرار أسئلة المحور الثالث السؤال الثامن

بلغت نسبة اجابات المبحوثين للسؤال الثامن على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٦٪ بعدد بلغ ٣٣ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٨٪ بعدد بلغ ١٤ شخص من نسبة المبحوثين، وحازت الاجابة (محايد) على النسبة الثالثة بمعدل بلغ ٦٪ بعدد بلغ ٣، وهذا يدل على إجماع عالي على انه تحتوي الشبكة على جدار ناري يحمي الشبكة من الاختراق بنسبة عالية بلغت ٩٤٪ من إجابات المبحوثين.

السؤال التاسع: يتم تثبيت مضادات الفيروسات والتحديثات الدورية

التكرار	النسبة المئوية	النسبة التراكمية	
٣٤	٦٨	٦٨	موافق جدا
١٤	٢٨	٩٦	موافق
١	٢	٩٨	محايد
١	٢	١٠٠	غير موافق
٥٠	١٠٠		الاجمالي

جدول ٣١ نسبة تكرار أسئلة المحور الثالث السؤال التاسع



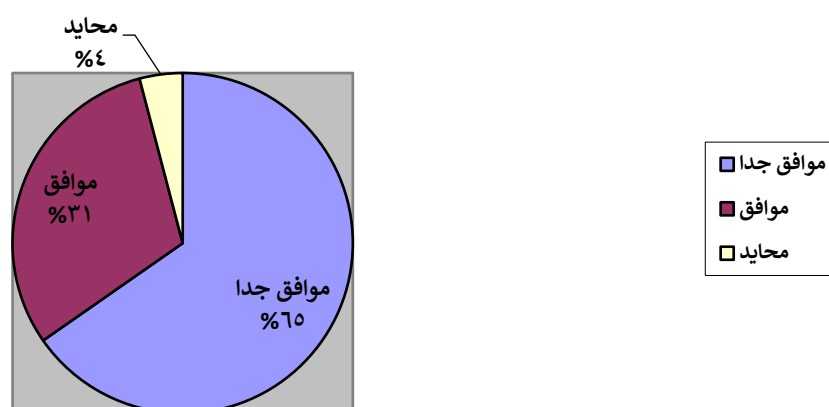
رسم توضيحي ٢٧ نسبة تكرار أسئلة المحور الثالث السؤال التاسع

بلغت نسبة اجابات المبحوثين للسؤال التاسع على فقرة (موافق جدا) على النسبة الاعلى بمعدل ٦٨٪ بعدد بلغ ٣٤ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٢٨٪ بعدد بلغ ١٤ شخص من نسبة المبحوثين، وحازت الاجابة (محايد - غير موافق) على إجابة واحدة فقط بنسبة بلغت ٢٪، وهذا يدل على إجماع كامل على موافقة المبحوثين على انه يتم تثبيت مضادات الفيروسات والتحديثات الدورية بنسبة موافقة كبيرة بلغت ٩٦٪ من إجابات المبحوثين.

السؤال العاشر: يتم صيانة الشبكة والعتاد دورياً

النسبة التراكمية	النسبة المئوية	التكرار	
٦٤	٦٤	٣٢	موافق جداً
٩٤	٣٠	١٥	موافق
٩٨	٤	٢	محايد
١٠٠	٢	١	غير موافق
	١٠٠	٥٠	الاجمالي

جدول ٣٢ نسبة تكرار أسئلة المحور الثالث السؤال العاشر



رسم توضيحي ٢٨ نسبة تكرار أسئلة المحور الثالث السؤال العاشر

بلغت نسبة اجابات المبحوثين للسؤال العاشر على فقرة (موافق جداً) على النسبة الاعلى بمعدل ٦٤٪ بعدد بلغ ٣٢ من نسبة المبحوثين وحازت الاجابة (موافق) على النسبة الثانية بمعدل ٣٠٪ بعدد بلغ ١٥ شخص من نسبة المبحوثين، وحازت الإجابة محايد على نسبة ٤٪ وعدد ٢ اجابات وحازت الاجابة (غير موافق) على النسبة الاقل بنسبة بلغت ٢٪ بعدد بلغ ١ وهذا يدل على إجماع كامل على موافقة المبحوثين على انه يتم صيانة

الشبكة والعتاد بشكل دوري، بنسبة موافقة كبيرة بلغت ٩٤٪ من إجابات المبحوثين.

سادساً: معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الأول عبر برنامج التحليل الإحصائي (SPSS)

م	الاسئلة	المتوسط الحسابي	الانحراف المعياري
١	يتم مراجعة وتطوير سياسة امن المعلومات بشكل دوري.	١,٦٤	٠,٦٩٣
٢	يتم إدخال المعلومات والبيانات بعد المصادقة من المدير المباشر.	١,٨٦	٠,٩٢٦
٣	لا يسمح لغير المختصين بالوصول إلى أجهزة الحاسب والعتاد المحوسب.	١,٤٢	٠,٨٣٥

٤	يمنع الدخول لمواقع الانترنت بالأجهزة الموصول بالخادم المركزي	١,٨٨	٠,٩١٨
٥	لا يسمح بتثبيت البرامج غير المرخصة والمقرصنة.	١,٤٤	٠,٨٣٧
٦	يتم التصريح بعناوين الحواسيب IP حتى يتم دخول النظام.	١,٨٦	٠,٩٠٤
٧	تسجيل أي عملية أثناء المعالجة باسم الموظف الذي قام بها مع التوقيت.	١,٥٤	٠,٧٦٢

جدول ٣٣ معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الأول

سابعاً: معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الثاني عبر برنامج التحليل الاحصائي (SPSS)

م	الاسئلة	المتوسط الحسابي	الانحراف المعياري
١	يتم تدريب العاملين على نظم الحوسبة بشكل دوري لتطويع مهاراتهم المتعلقة بالمستجدات الأمنية.	١,٥٨	٠,٧٣١
٢	يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة	١,٥٠	٠,٩٥٣

		تخص المؤسسة كجزء من شروط التوظيف.	
٣	١,٤٦	٠,٧٦٢	يطلب من الموظفين والمتعاقدين الإبلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.
٤	١,٦٦	٠,٩١٧	هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.
٥	١,٤٨	٠,٩٣١	يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة.
٦	١,١٦	٠,٦١٨	لكل موظف كلمة السر الخاصة به.
٧	١,٤٤	٠,٧٦٠	يطلب تغيير كلمة السر الخاصة بالموظف دورياً.
٨	١,٥٦	٠,٧٣٣	توجد مراجعة دورية لصلاحيات المستخدمين للوصول إلى الأنظمة.

جدول ٣٤ معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الثاني

ثامنا: معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الثالث عبر برنامج التحليل الاحصائي (SPSS)

م	الاسئلة	المتوسط الحسابي	الانحراف المعياري
١	تستخدم المؤسسة شتى الوسائل (أبواب - أقفال - بطاقات دخول - كاميرات) لحماية مكونات الأنظمة المعلوماتية.	١,٣٦	٠,٦٦٣
٢	يوجد في المؤسسة مصدر بديل للكهرباء إذا تم انقطاعها.	١,٣٤	٠,٦٢٦
٣	يمنع الموظف الغير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات.	١,٤٨	٠,٩٣١
٤	كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم خدمات الأنظمة المعلوماتية محمية من العبث بها أو إتلافها.	١,٥٠	٠,٨٣٩
٥	تستخدم طرق تشفير لحماية البيانات.	١,٤٨	٠,٨٦٣
٦	توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات وفي مكان آمن.	١,٥٤	٠,٨٣٨
٧	توجد برامج حماية لتتبع ومنع الاختراق والتسلل.	١,٤٢	٠,٧٨٥
٨	تحتوي الشبكة على جدار ناري يحمي الشبكة من الاختراق.	١,٤٠	٠,٦٠٦

٩	يتم تثبيت مضادات الفيروسات والتحديثات الدورية.	١,٣٨	٠,٦٣٥
١٠	يتم صيانة الشبكة والعتاد دورياً.	١,٤٤	٠,٦٧٥

جدول ٣٥ معدل المتوسط الحسابي والانحراف المعياري لإجابات المبحوثين للمحور الثالث

تاسعاً: اختبار فرضية الدراسة

وفي هذا الجدول مصفوفة معامل الارتباط بيرسون بين المتغير المستقل والتابع، حيث يمثل ثقة بمقدار ٩٥٪ كما هو موضح بالشكل الآتي:

Bootstrap Specifications

Sampling Method	Simple
Number of Samples	1000

Confidence Interval Level	95.0%
Confidence Interval Type	Percentile

جدول 23 معامل الارتباط بيرسون بين المتغير المستقل والتابع

Variable ١-٢		
	Pearson Correlation	٠,٤٤٠
	Sig. 2-tailed	٠,٢٧
.**Correlation is significant at the 0.01 level (2-tailed)		

جدول ٢٤ معامل الارتباط بيرسون بين المتغير المستقل والتابع

يتضح من الجدول السابق وجود علاقة ارتباط طردية ذات تأثير إيجابي للمتغير المستقل والمتغير التابع، وهي علاقة معنوية نظرا لانخفاض قيمة مستوى الدلالة عن ١٪ كما هو موضح نجمتين فوق كل قيمة لمعامل الارتباط

الفصل الرابع

النتائج والتوصيات

مقدمة

تم في هذا الفصل مناقشة النتائج والتوصيات في ضوء ما اسفرت عنه عملية التحليل الاحصائي لإجابات افراد العينة على فقرات متغيرات الدراسة، وذلك بهدف استخدام دور الامن السيبراني في حماية الأنظمة المعلوماتية.

أولا النتائج

١ الإدارة الجيدة في استخدام تكنولوجيا المعلومات يساهم بدرجة كبيرة في رفع دور الامن السيبراني في حماية الأنظمة المعلوماتية من خلال مواكبة التطور التكنولوجي عبر البرامج الجديدة والحديثة.

٢ تكنولوجيا المعلومات مهمة جدا في بناء وحماية الأنظمة المعلوماتية مع تطور وتعقيد العمليات وصعوبة مراقبتها، لذا أصبح من اللازم مواكبة تكنولوجيا المعلومات لتسهيل وتسريع عملية رقابة وحماية الأنظمة المعلوماتية.

٣ تبين انه يتم مراجعة وتطوير سياسة امن المعلومات بشكل دوري وهذا ينعكس إيجابا على دور الامن السيبراني في حماية الأنظمة المعلوماتية.

٤ تبين انه هناك رقابة مباشرة على ادخال البيانات والمعلومات من المدراء على الموظفين وهذا ينعكس إيجابا في دور الامن السيبراني في حماية الأنظمة المعلوماتية.

٥ لكفاءة العمال دور مهم في الحفاظ في حماية الأنظمة المعلوماتية.

٦ الدورات التدريبية للموظفين تساهم بشكل كبير في الحماية لنظم المعلومات.

٧ كلما زاد استخدم ادوت التكنولوجيا الحديثة في حماية الأنظمة المعلوماتية أدى ذلك إلى الزيادة في الحفاظ على امن الأنظمة المعلوماتية.

٨ يجب على المؤسسات تحفيز الموظفين وعمل ورش ودورات تدريبية بشكل دوري للحفاظ على الأنظمة المعلوماتية.

٩ يجب على المؤسسات عمل مكافآت عينية للموظفين في حال العثور على ثغرات أمنية للحد من خطورتها.

١٠ يجب على المؤسسات العمل بشكل مكثف على الصيانة الدورية للشبكات والعتاد.

١١ يجب على المؤسسات العمل في تثبيت وتحديث مضادات الفيروسات بشكل دوري.

١٢ يجب على المؤسسات العمل بشكل دوري على تحديث برامج الحماية لتتبع ومنع الاختراق والتسلل للحد من خطورتها.

١٣ يجب على المؤسسات تغيير كلمة السر للموظفين بشكل دوري.

ثانياً التوصيات:

- ١ العمل على اتباع نهج فعال في حماية المعلومات والبيانات لوضع حد امام مقرصني المعلومات من الوصول إلى المعلومات.
- ٢ توفير برامج وورش تدريبية متخصصة بأمن نظم المعلومات للأفراد العاملين في نفس المجال.
- ٣ توعية الموظفين والعاملين بمخاطر استخدام الأجهزة الشخصية مثل الهاتف المحمول لتخزين او نقل معلومات سرية خاصة بالمؤسسة.
- ٤ منح الموظفين حوافر مادية ومعنوية للمبدعين في مجال الامن السيبراني.

- ٥ اهتمام الشركات الكبرى في إدارة امن المعلومات واعتباره عنصراً إلزامياً على قائمة اعمالها.
- ٦ عمل منصات توعوية ومعرفة وذلك لتعزيز أهمية الامن السيبراني في المملكة ككل.
- ٧ عمل ورش ودورات في تدقيق نظم المعلومات وتحسين كفاء نظم المعلومات.
- ٨ عمل ورش ودورات في إدارة الازمات الالكترونية.
- ٩ عمل دورات في تطبيق المعايير الدولية لأمن المعلومات.
- ١٠ عمل دورات في أمن الأنظمة.
- ١١ عمل دراسات شاملة والاهتمام في موضوع الامن السيبراني.
- ١٢ تطوير البنية التحتية السيبرانية في المملكة للحد من الاختراق والتجسس والقرصنة الالكترونية.

الفصل الخامس

المراجع والملحقات

المراجع

المراجع باللغة العربية:

١. ابراهيم رمضان عطايا. ٢٠١٥. الجريمة الالكترونية وسبل مواجهتها في التشريع الاسلامي والانظمة الدولية. القاهرة : مجلة كلية التشريع والقانون المجلد ٢٠ العدد ٢، ٢٠١٥.
٢. ابو موسى، احمد عبدالسلام وخطاب، محمد شحاته. ٢٠١٢. عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات.

الرياض : مجلة كلية تجارة للبحوث العلمية - كلية التجارة - جامعة الاسكندرية،
٢٠١٢.

٣. أحمد جلال محمود. ٢٠٢٠. أثر التهديدات غير التقليدية للأمن على العلاقات الدولية المعاصرة - الامن السيبراني في الشرق الاوسط. القاهرة : مركز الشرق الاوسط للدراسات المستقبلية، ٢٠٢٠.

٤. أشرف توفيق. ٢٠١٩. مخاطر العملات الافتراضية في نظر السياسة الجنائية. القاهرة : مطبعة اكتوبر، ٢٠١٩.

٥. اكرم محمد رضا الطويل. ٢٠١٥. التوزيع المادي وعناصر خدمة العميل. الاردن : دار الحامد للنشر - عمان الطبعة الاولى، ٢٠١٥.

٦. الرؤية العربية للأمن السيبراني. ٢٠٢١. الواقع - التحديات - الفرص. تونس : المنظمة العربية لتكنولوجيا الاتصال والمعلومات، ٢٠٢١.

٧. المركز الوطني للأمن السيبراني. ٢٠٢٤. الأمن السيبراني. الرياض : المركز الوطني للأمن السيبراني، ٢٠٢٤.

٨. الهيئة الوطنية للأمن السيبراني. ٢٠١٨. الاستراتيجية الوطنية للأمن السيبراني. الرياض : الهيئة الوطنية للأمن السيبراني في المملكة، ٢٠١٨.

٩. الهيئة الوطنية للأمن السيبراني. ٢٠١٨. الضوابط الاساسية للأمن السيبراني. ٢٠١٨.

١٠. أيمن البوغانمين. ٢٠١٩. بنية سوق المعلومات في عصر الانترنت. مكان غير معروف : مجلة الباب العدد ١٤، ٢٠١٩.

١١. بدر الحيمودي. ٢٠٢٣. الامن السيبراني وحماية الانظمة المعلوماتية. المغرب : مجلة شمال افريقيا للنشر العلمي العدد الاول الطبعة الاولى، ٢٠٢٣. ٢٩٥٩-٤٨٢٠.

١٢. بن عليّة بن جدو. ٢٠٢٢. تحديات الامن السيبراني لمواجهة الجريمة الالكترونية. بومرداس : المجلة الجزائرية للأمن السيبراني - السنة السابعة - المجلد ٧ - العدد ٢، ٢٠٢٢. ٢٦٧٦-١٦٤٥.

١٣. حمدي محمد محمود حسين. ٢٠١٨. المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي. برلين : مجلة العلوم السياسية والقانون المركز الديمقراطي العربي، المجلد ٢، العدد ٨، ٢٠١٨.
١٤. خالد ممدوح ابراهيم. ٢٠١٨. حجية البريد الإلكتروني في الإثبات دراسة مقارنة. الاسكندرية : دار الفكر الجامعي الطبعة الأولى، ٢٠١٨.
١٥. د. الجوهرة بنت عبدالرحمن ابراهيم المنيع. ٢٠٢٢. متطلبات تحقيق الامن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠. جدة : إدارة البحوث والنشر العلمي (المجلة العلمية) المجلد الثامن والثلاثون - العدد الاول - يناير ٢٠٢٢، ٢٠٢٢.
١٦. د. رضا ابراهيم صالح. ٢٠٢٠. دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات الحاسوبية. مكان غير معروف : مجلة الدراسات التجارية المعاصرة ١٠٧ المجلد السادس - العدد العاشر الجزء الأول، ٢٠٢٠.
١٧. د. شريهان مصطفى التوني. ٢٠٢٣. أثر وعي العملاء بالقرصنة الالكترونية كأداة لتحقيق الأمن السيبراني. بورسعيد : المجلة العلمية للتجارة والتمويل - العدد الرابع، ٢٠٢٣.
١٨. د.راشد محمد المري. ٢٠٢٤. الامن السيبراني وحماية الانظمة الالكترونية. جدة : مجلة الدراسات القانونية والاقتصادية - دورية علمية محكمة، ٢٠٢٤. ٩٤٩٢-٢٣٥٦.
١٩. زينب طرفي العنزي. ٢٠٢٢. الجريمة الالكترونية في ميزان الفقه والقانون. العراق : مجلة الدراسات الاسلامية والبحوث، ٢٠٢٢.
٢٠. سامي سعد السميري. ٢٠٢٢. واقع الامن السيبراني وتحدياته في السعودية. جدة : المجلة العلمية لجامعة الملك فيصل - العدد ١ - مجلد ٢٣، ٢٠٢٢.
٢١. سمير قلاع ضرورسو. ٢٠٢٢. الامن السيبراني الوطني قراءة في أهم الاستراتيجيات الامنية لمواجهة الجريمة الالكترونية بالجزائر. الجزائر : مجلة الرواق للدراسات الاجتماعية والسياسية مجلد ٨ - عدد ٢، ٢٠٢٢.
٢٢. شبيخة حسن الزهراني. ٢٠٢٣. التعاون الدولي في مواجهة الهجوم السيبراني. مكان غير معروف : دار الفكر العربي للنشر والتوزيع الطبعة الثالثة العدد ١٢، ٢٠٢٣.

٢٣. شيماء مرزوق. ٢٠٢٤. إنعكاسات الامن السيبراني على أمن المعلومات في البنوك. تبسة : جامعة الشهيد الشيخ العربي التبسي، ٢٠٢٤.
٢٤. عادل موسى عوض. ٢٠٢٢. وسائل حماية الامن السيبراني - دراسة فقهية تأصلية مقارنة بالنظم المعاصرة. القاهرة : جامعة الازهر كلية الشريعة والقانون المجلة العلمية العدد ٢٤ الاصدار الاول الجزء الثالث، ٢٠٢٢.
٢٥. عبدالفتاح بيومي حجازي. ٢٠١٩. النظام القانوني للحكومة الالكترونية. الاسكندرية : دار الفكر الجامعي الكتاب الاول، ٢٠١٩.
٢٦. عزة فاروق جوهرى. ٢٠٢٣. أمن المعلومات الرقمية وسبل حمايته في ظل التشريعات الراهنة. القاهرة : مجلة المركز العربي للبحوث والدراسات في علوم المكتبات والمعلومات المجلد ٦ العدد ١٢، ٢٠٢٣.
٢٧. علاء الدين فرحات. ٢٠٢١. من الردع النووي إلى الردع السيبراني دراسة لمدة تحقيق مبدأ الردع في الفضاء السيبراني. الجزائر : مجلة الفكر المجلد ١٦ العدد ١، ٢٠٢١.
٢٨. علي حسن طوال. ٢٠٢٤. مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي، دراسة مقارنة . الاردن : مركز الاعلام الامني، ٢٠٢٤.
٢٩. علي زايد محمد الجبيري الشهري. ٢٠١٩. الاطار القانوني للحد من الجرائم الالكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية. جدة : كلية العلوم الاستراتيجية قسم الدراسات الاستراتيجية، ٢٠١٩.
٣٠. غريب جبر جبر. ٢٠٢٣. تهديدات الامن السيبراني للمصارف الالكترونية وآلية مواجهاتها. طنطا : المجلة الاكاديمية للعلوم الاجتماعية مجلد ١ عدد ١، ٢٠٢٣.
٣١. م.م. فاطمة علي. ٢٠٢٢. الامن السيبراني والنظافة الرقمية. القاهرة : المجلة المصرية لعلوم المعلومات المجلد ٩ العدد ٢، ٢٠٢٢.
٣٢. محمد بن مرزوق. ٢٠١٨. البعد الالكتروني للسياسة الامنية الجزائرية في مكافحة الارهاب. الجزائر : مجلة العلوم الانسانية والاجتماعية جامعة الحاج لخضر عدد ٣٨، ٢٠١٨.
٣٣. مزيان عبدالقادر. ٢٠١٧. أثر محددات جودة العملاء على رضى العملاء. الجزائر : جامعة تلمسان، ٢٠١٧.

٣٤. وليد الزبيدي. ٢٠٢١. القرصنة على الانترنت والحاسوب. عمان : دار اسامة للنشر الطبعة الثالثة، ٢٠٢١.

المراجع باللغة الانجليزية:

- 1- A.R Warman .٢٠١٣ .Computer Security Within Organization :.Macmillan Press, Basing Stock, ٢٠١٣ ،
- 2- T., Kiountouzis, E & .Poulymenakou, Tryfonas .٢٠٠١ .Embedding Security Practices in Contemporary Information Systems Development Approaches :. Information Management &Computer Security, Vol. 9, No. 4..٢٠٠١ ،

المراجع الالكترونية:

- هيئة الحكومة الرقمية. ٢٠٢٤. <https://www.cst.gov.sa/ar/Digitalknowledge/Pages/cyber-security.aspx> [متصل] ٨١ ، ٢٠٢٤. [تاريخ الاقتباس: ٨١ ، ٢٠٢٤].
- وزارة الموارد البشرية. ٢٠٢٤. <https://www.hrsd.gov.sa/729863> [متصل] ٥ يونيو، ٢٠٢٤. [تاريخ الاقتباس: ٨١ ، ٢٠٢٤].
- شهيره دعوى. ٢٠١٦. https://mawdoo3.com/%D9%85%D9%81%D9%87%D9%88%D9%85_%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D8%A7%D8%AA [متصل] ٢٣ اغسطس، ٢٠١٦. [تاريخ الاقتباس: ٨١ ، ٢٠٢٤].
- رؤى حمود. ٢٠٢٤. <https://www.rmg-sa.com/6-%D9%85%D9%86-%D8%A3%D9%87%D9%85-%D8%A3%D8%AF%D9%88%D8%A7%D8%AA-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A> [متصل] ٨١ ، ٢٠٢٤. [تاريخ الاقتباس: ٨١ ، ٢٠٢٤].

الاستبانة:

1.البيانات الشخصية:

• العمر :

- ☐ أقل من ١٨ عامًا
- ☐ 18-24 عامًا
- ☐ 25-34 عامًا
- ☐ 35-44 عامًا
- ☐ 45-54 عامًا
- ☐ 55 عامًا أو أكثر

• الجنس :

- ☐ ذكر
- ☐ أنثى

• التعليم :

- ☐ الثانوية العامة
- ☐ دبلوم
- ☐ بكالوريوس
- ☐ دراسات عليا

٢- المحور الأول: السياسات والجراءات

السؤال	موافق وبشدة	موافق	محايد	غير موافق	غير موافق وبشدة
١- يتم مراجعة وتطوير سياسة امن المعلومات بشكل دوري.					
٢- يتم إدخال المعلومات والبيانات بعد المصادقة من المدير المباشر.					
٣- لا يسمح لغير المختصين بالوصول إلى أجهزة الحاسب والعتاد المحوسب.					
٤- يمنع الدخول لمواقع الانترنت بالأجهزة الموصول بالخادم المركزي					
٥- لا يسمح بتثبيت البرامج غير المرخصة والمقرصنة.					
٦- يتم التصريح بعناوين الحواسيب IP حتى يتم دخول النظام.					
٧- تسجيل أي عملية أثناء المعالجة باسم الموظف الذي قام بها مع التوقيت.					

المحور الثاني: إجراءات امن المعلومات المتعلقة بالعاملين

السؤال	موافق وبشدة	موافق	محايد	غير موافق	غير موافق وبشدة
١- يتم تدريب العاملين على نظم المحوسبة بشكل دوري لتطوير مهاراتهم المتعلقة بالمستجدات الأمنية.					
٢- يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص المؤسسة كجزء من شروط التوظيف.					
٣- يطلب من الموظفين والمتعاقدين الإبلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.					
٤- هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.					
٥- يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة.					
٦- لكل موظف كلمة السر الخاصة به.					
٧- يطلب تغيير كلمة السر الخاصة بالموظف دورياً.					
٨- توجد مراجعة دورية لصلاحيات المستخدمين للوصول إلى الانظمة					

المحور الثالث: إجراءات امن المعلومات المتعلقة بالعتاد والبيانات

السؤال	موافق وبشدة	موافق	محايد	غير موافق	غير موافق وبشدة
١- تستخدم المؤسسة شتى الوسائل (أبواب – أقفال – بطاقات دخول – كاميرات) لحماية مكونات الأنظمة المعلوماتية.					
٢- يوجد في المؤسسة مصدر بديل للكهرباء إذا تم انقطاعها.					
٣- يمنع الموظف الغير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات.					
٤- كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم خدمات الأنظمة المعلوماتية محمية من العبث بها أو إتلافها.					
٥- تستخدم طرق تشفير لحماية البيانات.					
٦- توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات وفي مكان آمن.					
٧- توجد برامج حماية لتتبع ومنع الاختراق والتسلل.					
٨- تحتوي الشبكة على جدار ناري يحمي الشبكة من الاختراق.					

٩-	يتم تثبيت مضادات الفيروسات والتحديثات الدورية.				
١٠-	يتم صيانة الشبكة والعتاد دورياً.				

الملخص باللغة العربية

اهتمت مشكلة الدراسة بالتعرف على ما هو دور الامن السيبراني في حماية الأنظمة المعلوماتية وماهي طرق تطوير دور الامن السيبراني في حماية الأنظمة المعلوماتية وهدفت الدراسة إلى التعرف على واقع دور الامن السيبراني في حماية الأنظمة المعلوماتية والتعرف على أساليب تطوير حماية الأنظمة المعلوماتية والثغرات والتعرف على آراء واخطاء العاملين في نفس المجال واتبعت منهجية الدراسة على المنهج الوصفي التحليلي وذلك من خلال تصميم استبانة وتوزيعها وتحليلها في برنامج التحليل الاحصائي SPSS وتكون مجتمع البحث من عينة عشوائية توزعت على بعض العاملين في مجال الامن السيبراني وبينت نتائج الدراسة على أنه الإدارة الجيدة في استخدام تكنولوجيا المعلومات يساهم بدرجة كبيرة في رفع دور الامن السيبراني في حماية الأنظمة المعلوماتية من خلال مواكبة التطور التكنولوجي عبر البرامج الجديدة والحديثة.

الكلمات المفتاحية:

الأمن السيبراني، الأنظمة المعلوماتية.

Abstract:

The study problem was concerned with identifying the role of cybersecurity in protecting information systems and what are the ways to develop the role of cybersecurity in protecting information systems. The study aimed to identify the reality of the role of cybersecurity in protecting information systems and to identify the methods of developing the protection of information systems and loopholes and to identify the opinions and mistakes of workers in the same field. The study methodology followed the descriptive analytical approach by designing a questionnaire, distributing it and analyzing it in the statistical analysis program SPSS. The research community consisted of a random sample distributed among some workers in the field of cybersecurity. The results of the study showed that good management in the use of information technology contributes greatly to raising the role of cybersecurity in protecting information systems by keeping pace with technological development through new and modern programs.

Keywords:

Cybersecurity, Information Systems.

Midocean University

College of Management

Department of Risk Management



Project Title:

The role of cybersecurity in protecting information systems

Prepared by:

Sultan Suliman Ojaymi

٢٣٣...٢٠٢

Supervised by:

Dr. AlFaisal Abdul Hamid

Dr. Fayez Jarad

Year:2024