الجمهورية الجزائرية الديمقراطية الشعبية

و زارة التعليم العالي والبحث العلمي

جامعـــة محمـد خيضر– بسكـــرة-

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلوم الاقتصادية

الموضوع

دور الأمن السيبراني في تحسين البيئة الرقمية

دراسة حالة جامعة محمد خيضر بسكرة

مذكرة مقدمة كجزء من متطلبات نيل شهادة الماستر في العلوم الاقتصادية.

تخصص: اقتصاد رقمي.

إعداد الطالبة:

– أميرة ندى الريحان سماتي.

الأستاذ المشرف:

– عبد الرزاق بن الزاوي.

لجنة المناقشة

اعضاء اللجنة	الرتبة	الصفة	الجامعة
– عمر قريد	– أستاذ	رئيسا	بسكرة
– عبد الرزاق بن الزاوي	– أستاذ	مقررا	بسكرة
– انصاف قسوري	– أستاذ	مناقشا	بسكرة

الموسم الجامعي: 2025/2024

الجمهورية الجزائرية الديمقراطية الشعبية

و زارة التعليم العالي والبحث العلمي

جامعـــة محمـد خيضر– بسكـــرة-

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلـــوم الاقتصادية

الموضوع

دور الأمن السيبراني في تحسين البيئة الرقمية

دراسة حالة جامعة محمد خيضر بسكرة

مذكرة مقدمة كجزء من متطلبات نيل شهادة الماستر في العلوم الاقتصادية.

تخصص: اقتصاد رقمي

إعداد الطالبة:

– أميرة ندى الريحان سماتي.

الأستاذ المشرف:

– عبد الرزاق بن الزاوي.

لجنة المناقشة

اعضاء اللجنة	الرتبة	الصفة	الجامعة
– عمر قريد	– أستاذ	رئيسا	بسكرة
– عبد الرزاق بن الزاوي	– أستاذ	مقررا	بسكرة
– انصاف قسوري	– أستاذ	مناقشا	بسكرة

الموسم الجامعي: 2025/2024


بسم الله الرحمن الرحيم

الشكر و العرفان

بسم الله الرحمن الرحيم

﴿ وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ ﴾

الحمد لله الذي وفقني وأعانني، وأسبغ عليّ من نعمه الظاهرة والباطنة، وأسأله جلّ في علاه أن يجعل هذا العمل خالصًا لوجهه الكريم، وأن ينفع به، إنه وليّ ذلك والقادر عليه.

أتقدّم بجزيل الشكر وخالص الامتنان إلى أستاذي الكريم الدكتور/ الأستاذ الفاضل " بن الزاوي عبد الرزاق "، الذي لم يبخل عليّ بعلمه وخبرته، وكان دعمُه المتواصل وتوجيهه السديد منارات أضاءت لي الطريق طوال فترة إعداد هذا العمل. فله مني كل الشكر والتقدير.

ولا يفوتني أن أعبّر عن عظيم امتناني لأعضاء لجنة المناقشة الأفاضل، الذين شرفوني بقراءتهم لهذا العمل، وملاحظاتهم التي سأحرص كل الحرص على الاستفادة منها في المستقبل.

كما أرفع أسمى عبارات الشكر والعرفان إلى كافة أساتذتي في كلية العلوم الاقتصادية والتجارية وعلوم التسيير، الذين تركوا فينا بصمات لا تُنسى، وغرسوا فينا حبّ المعرفة والبحث.

ولكل من دعمني، ولو بكلمة طيبة أو دعوة صادقة، من قريب أو بعيد، فلكم في قلبي مكان، ولكم مني كل الشكر والتقدير، وأسأل الله أن يوفقنا جميعًا لما فيه الخير والنجاح. والله وليّ التوفيق.

وشكرا

الإهداء

أتوجه بخالص الشكر والامتنان إلى والديَّ العزيزين، أمي وأبي، على ما قدّماه لي من دعم متواصل، ومحبة لا تُقدّر بثمن. فأنتم السند الحقيقي في حياتي، ومصدر القوة والإلهام في كل خطوة

كما لا يفوتني أن أعبّر عن محبتي العميقة لأخواتي الغاليتين وصال وأريج، ولأخي الوحيد ورفيق دربي أنيس العزيز، الذي يستحق شكرًا خاصًا لمساندته المستمرة، ووقوفه إلى جانبي في كل الظروف.

شكر عميق ومليء بالامتنان أقدّمه إلى خالتي العزيزة وهيبة، التي لم تبخل عليّ بالدعم والمساندة، وكانت دومًا من المساندين الحق... كما لا يفوتني أن أتوجه بخالص الشكر والامتنان إلى أفراد هذه العائلة الكريمة، وخاصّة أولادها الأعزاء، الذين كانوا لي خير سند في مشواري.

وأخص بالذكر إسلام شكال، الأقرب إلى قلبي، الذي لم يتوانَ لحظة في دعمي ومساندتي، وكان دوما حاضرًا بقلبه الكبير ونبله المعهود.

كما أشكر رائد، وعبد الكريم، وزكريّا، والكتكوتة الصغيرة أسينات،

ولا ننسى زوج خالتي الخلوق ماليك شكّال، على دعمهم المتواصل وطيبة معدنهم وصفاء سيرتهم.

ولا يفوتني أن أخصّ بالشكر خالي دعّاس حسام الدين، الذي كان دومًا في ظهري، يشجعني ويساندني دون كلل، الذي كان لنا سندًا في جميع المواقف، لم يبخل علينا بعطائه، فجزاه الله خير الجزاء، وأصلح له أولاده، وجعلهم من الذرية الصالحة.

أخص بالشكر والتقدير ابن عمي العزيز البروفيسور حاتم سماتي، على مجهوداته القيّمة، ومساهمته التي أعتز بها كثيرا، فقد كان له دور فعّال في إنجاح هذا العمل.

كما لا أنسى أن أقدّم تحية محبة وشكر لصديقتي العزيزتين فاتن وعواطف، منار على الونس والضحكة والدعم الصادق خلال كل المراحل الدراسية

كما لا أنسى أن أقدّم تحية إلى قطي العزيز، الذي كان رفيقي الصامت في ساعات العمل الطويلة، بوجوده منحني طاقة إيجابية وهدوءا ساعداني على مواصلة هذا الجهد.

له كل الامتنان، فقد كان جزءا من رحلتي في إنجاز هذا العمل.

أميرة

ملخص الدراسة

هدفت هذه الدراسة إلى معرفة دور الأمن السيبراني في تحسين البيئة الرقمية بجامعة محمد خيضر بسكرة. ولتحقيق أهداف البحث، تم استخدام استمارة لجمع البيانات وزعت على عينة مكونة من 50 أستاذا واسترجعنا منها 36 استبانة، كما تم اعتماد برنامج SPSS لإجراء التحليل الإحصائي للبيانات.

توصلت الدراسة إلى مجموعة من النتائج المهمة، أبرزها وجود أثر واضح وفعال للأمن السيبراني في تحسين البيئة الرقمية بالجامعة، عند مستوى دلالة إحصائية معتبر. حيث أظهرت النتائج أن الأمن السيبراني يمثل عنصرًا أساسيا ومتكاملا في تحسين البيئة الرقمية، من خلال المساهمة في رفع كفاءة الخدمات الجامعية، وضمان حماية المعطيات، وتعزيز ثقة الأساتذة في استخدام الوسائط الرقمية، مما يعكس الدور الاستراتيجي الذي يلعبه الأمن السيبراني في دعم التحول الرقمي وتشجيع الابتكار داخل المؤسسات التعليمية.

كما اقترحت الدراسة مجموعة من التوصيات، من أهمها وضع استراتيجية مؤسساتية واضحة للأمن السيبراني تشمل التكوين المستمر، وتحديث الأنظمة، وتطوير آليات الاستجابة للطوارئ، إلى جانب تعزيز التوعية الرقمية لدى الطلبة والموظفين من خلال تنظيم دورات تكوينية منتظمة حول المخاطر السيبرانية وسبل الوقاية منها.

- **الكلمات المفتاحية : الامن السيبراني، التهديدات السيبرانية، البيئة الرقمية ، الرقمنة.**

Abstract:

This study aimed to investigate the role of cybersecurity in improving the digital environment at Mohamed Khider University of Biskra. To achieve the research objectives, a questionnaire was used to collect data from a sample of 50 professors, and the SPSS software was employed for statistical data analysis.

The study yielded several important findings, the most notable of which is the clear and effective impact of cybersecurity on enhancing the university's digital environment, with a statistically significant level of confidence. The results showed that cybersecurity constitutes a fundamental and integral component in improving the digital environment by contributing to the efficiency of university services, ensuring data protection, and boosting professors' confidence in using digital platforms. This highlights the strategic role of cybersecurity in supporting digital transformation and fostering innovation within educational institutions.

The study also proposed a set of recommendations, most notably the need to establish a clear institutional cybersecurity strategy that includes continuous training, system updates, and the development of emergency response mechanisms. Additionally, it emphasized the importance of raising digital awareness among students and staff through the organization of regular training sessions on cyber risks and prevention methods.

- **Keywords: Cybersecurity, Cyber Threats, Digital Environment, Digitization**.

قائمة الجداول

قائمة الاشكال

مقدمة

شهد العالم في العقود الأخيرة تحوّلاً جذريًا بفعل الثورة التكنولوجية والمعلوماتية، التي غيّرت معالم الحياة في مختلف المجالات، لاسيما في قطاع الاقتصاد والتعليم والإدارة. فقد أدى التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصالات إلى انتقال المجتمعات من نمط الاقتصاد الصناعي التقليدي إلى ما يعرف اليوم بـ"الاقتصاد الرقمي"، القائم على المعرفة والمعلومة كأهم موارد القوة والإنتاج، بدلا من الاعتماد على الموارد الطبيعية وحدها.

وفي ظل هذا التحول الرقمي، أصبحت شبكة الإنترنت من أهم الوسائل التي مكنت من تسريع وتيرة التبادل المعلوماتي، وساهمت في إعادة تشكيل مختلف القطاعات، على غرار التجارة، التعليم، الإدارة، والخدمات المالية، من خلال إدماج التطبيقات الرقمية الحديثة وتطوير أدوات الاتصال والتفاعل.

غير أن هذا الانتقال إلى البيئة الرقمية لم يخل من تحديات ومخاطر، لعل أبرزها تلك المرتبطة بأمن المعلومات وحماية الأنظمة الرقمية. فمع تزايد الاعتماد على البيانات والأنظمة الإلكترونية، برزت الحاجة الملحّة إلى تأمين البنى التحتية الرقمية والتصدي للتهديدات السيبرانية التي قد تمس بسرية المعلومات، سلامتها، وتوافرها.

ومن هنا، بات الأمن السيبراني يشكل أحد المحاور الجوهرية في السياسات الرقمية الحديثة، إذ لم يعد ينظر إليه كخيار تقني فقط، بل كضرورة استراتيجية لحماية الأفراد والمؤسسات على حد سواء. وتشكل المؤسسات الجامعية، باعتبارها فضاءات معرفية تعتمد بشكل متزايد على الأنظمة الإلكترونية في تسيير مهامها الأكاديمية والإدارية، إحدى البيئات التي تواجه تحديات متزايدة في هذا المجال.

وفي هذا السياق، تأتي هذه الدراسة لتسلط الضوء على واقع الأمن السيبراني في البيئة الرقمية داخل الجامعات الجزائرية، من خلال دراسة حالة جامعة محمد خيضر بسكرة، بهدف رصد أبرز التحديات التي تعترض جهود الحماية الرقمية، وتحليل آليات التصدي لها، واقتراح سبل تعزيز أمن المعلومات في هذا الفضاء الأكاديمي الحيوي.

I. إشكالية الدراسة والأسئلة البحثية :

وعلى ضوء ما سبق يمكننا صياغة إشكالية البحث من خلال طرح التساؤل الرئيسي التالي:

- **ما هو دور الامن السيبراني في تحسين البيئة الرقمية بجامعة محمد خيضر بسكرة؟**

ولكي يتسنى لنا التطرق لمختلف جوانب الموضوع تم تجزئة الإشكالية إلى الأسئلة الفرعية التالية:

1. هل هناك دور للأمن السيبراني في تحسين البنى التحتية بجامعة محمد خيضر بسكرة؟
2. هل هناك دور بين للأمن السيبراني في تحسين المهارات الرقمية بجامعة محمد خيضر بسكرة ؟
3. هل هناك دور بين للأمن السيبراني في تحسين الثقافة الرقمية بجامعة محمد خيضر بسكرة ؟

II. دراسات سابقة:

من خلال عملية البحث، اتضح أن الموضوع يحتوي على مجموعة معتبرة من الدراسات السابقة تناولت موضوع الامن السيبراني أهميته في البيئة الرقمية، وذلك من عدة زوايا و مفاهيم مختلفة، منها ما تعلق ب الامن السيبراني وأدواته، ومنها ما تعلق بالبيئة الرقمية إلى غير ذلك من المواضيع، كما أن هذه الدراسات ساعدتنا كثيرا في توجيه هذه الدراسة وسنتطرق لهذه دراسات في ما يلي:

أولا: **دراسات تتعلق الامن السيبراني:**

- **الدراسة الأولى:** بدر عدنان احمد سعد الخبيزي. (03 09, 2023). تحديات وتهديدات الامن السيبراني وكيفية التغلب عليه. *حوليات آداب عين شمس، 51* ، جامعة عين الشمس، مصر، 230- 252 صفحة.

✓ يهدف إلى إلقاء الضوء علي ماهية الأمن السيبراني وذلك من حيث التعريف والأهداف والأهمية والفوائد. أيضا البحث يهدف إلى رصد بعض التحديات والتهديدات التي تواجه الأمن السيبراني في الوقت الحالي، وتقديم مجموعة من الإجراءات والتوصيات لكيفية التغلب علي هذه التحديات والتهديدات أو التخفيف من حدتها أو تقليل عددها.

✓ يقوم البحث على استخدام المنهج تم الاعتماد على المنهج الوصفي الذي يهدف إلى وصف الظاهرة موضوع البحث من خلال الكتابات والأدبيات (مثل: الكتب والبحوث والرسائل العلمية المتاحة عن الموضوع.

✓ وتوصلت الدراسة الى نتائج أهمها: إن الفضاء السيبراني أو الإلكتروني سلاح ذو حدين لما يتضمنه من إيجابيات من جهة ومن تحديات وتهديدات من جهة أخرى، ولا سيما أن الهجمات والجرائم السيبرانية أصبحت مركبة ومعقدة ومتسارعة وخطيرة ويصعب على الكثير من المؤسسات التغلب والدفاع عن أمنها السيبراني دون وجود إستراتيجيات عمل وطنية واقتناء تقنيات وتطبيقات متطورة وممارسات سليمة ضمن إستراتيجية شاملة.

ثانيا: دراسة تتعلق بالبيئة الرقمية.

- **الدراسة الثانية:** رحاب فايز احمد السيد، و عمر حوتيه. (30 03, 2023). المكتبات الجامعية الرقمية كانموذج للتحول نحو العمل في البيئة الرقمية. *مجلة ببليوفيليا للدراسات المكتبات والمعلومات*، جامعة العربي تبسي، تبسة، الجزائر،14-32صفحة .

✓ تهدف هذه الدراسة إلى تلبية احتياجات الباحثين والدارسين ورغبتهم في الحصول على معلومات سريعة وحديثة، مقابل عدم قدرة أنظمة المعلومات التقليدية على تلبيتها.

- التعريف بالتكنولوجيا الرقمية وتزايد استخداماتها في بيئة المكتبات الجامعية.
- تبيان مراحل ومتطلبات تحول المكتبات الجامعية من تقليدية إلى رقمية (إنشاء مكتبة جامعية رقمية).
- إبراز أوجه تأثير التكنولوجيا الرقمية في خدمات المكتبات الجامعية، والتحديات التي تواجه رقمنتها.

✓ اعتمدت الدراسة على المنهج الوصفي التحليلي، نظرا لكونه يقوم على جمع البيانات وتحليلها بطريقة موضوعية وعلمية، ويتلاءم مع طبيعة الدراسة التي تهدف إلى تسليط الضوء على المهام الجديدة للمكتبات الجامعية في ظل التحول نحو العمل في البيئة الرقمية.

✓ سمحت هذه الدراسة بالتوصل إلى نتائج أهمها:

- ان الرقمنة أحدثت ثورة في مفهوم المكتبات، حيث حولتها إلى مكتبات مفتوحة للجميع تعمل ضمن بيئة رقمية متغيرة.
- تبرز أهمية رقمنة المكتبات الجامعية في إتاحة الكتب ومصادر المعلومات الرقمية للمستفيدين، مما يساهم في تسريع الوصول إلى المعلومة داخل بيئة رقمية تضع المعرفة في متناول الباحثين.

- يمكن حصر التحول من مفهوم المكتبات التقليدية إلى المكتبات الرقمية في ثلاث مراحل رئيسية: مرحلة الإعداد والتجهيز، ومرحلة التنفيذ وإنجاز المشروع، ثم مرحلة إطلاق الخدمة.
- إن تطبيق مشاريع المكتبات الرقمية يعتمد على عدة عناصر يجب توافرها لضمان مقومات النجاح، ومن أبرزها ضرورة وجود خطة واضحة لرقمنه المكتبات.

ثالثا: دراسة تجمع المتغيرين معا "الامن السيبراني والبيئة الرقمية" :

- ✓ **الدراسة الثالثة:** عبد الجليل طواهير. (31 03, 2023). إستراتيجيات الأمن السيبراني كتحدي لتحول الرقمية بالمنظمات الحكومية مع الاشارة لتجربة دولة الإمارات العربية المتحدة. *مجلة الرسالة للدراسات الاعلامية، 7* . جامعة العربي تبسي، تبسة، الجزائر، 297-291صفحة .
- ✓ تهدف الدراسة الى التعرف على استراتيجيات الأمن السيبراني بالنظر إلى خطورة التهديدات التي يمثلها العدم الأمن الإلكتروني على الأفراد والمنظمات والدول و في ظل الحاجة المتزايدة لضرورة التحول الرقمي في خدمات المنظمات.
- ✓ اعتمدت هذه الدراسة على المنهج الوصفي، الذي يقوم على جمع المعلومات الحقائقية بهدف سرد الأفكار والمفاهيم، وهذا ما يعتبر مناسبا لطبيعة الموضوع.
- ✓ سمحت هذه الدراسة بالتوصل إلى نتائج أهمها:

- التحول الرقمي الشامل :يشهد العالم تزايدا ملحوظا في الاعتماد على خدمات الاتصالات والتكنولوجيا، مما يتطلب تعزيز البنية التحتية الرقمية وتأهيل العنصر البشري لمواكبة هذا التحول.
- ضرورة المعايير الأمنية :يفرض تسارع الجرائم الإلكترونية أهمية قصوى على تطبيق أعلى معايير الأمن السيبراني إلى جانب تشريعات قانونية واضحة، لمواجهة التحديات الرقمية المعقدة.
- دور الإمارات كنموذج ناجح :تعد الإمارات العربية المتحدة نموذجًا رائدا في تعزيز الأمن السيبراني، حيث تمكنت خلال عامين فقط من رفع تنافسيتها الدولية عبر تحسين استجابتها للتهديدات السيبرانية، ووضع سياسات وتشريعات فعالة لمكافحة الجرائم الإلكترونية.
- أهمية الوعي المجتمعي :الأمن السيبراني ليس مسؤولية الحكومات فقط، بل يبدأ من وعي الأفراد بصفتهم خط الدفاع الأول، مما يتطلب جهودا تكاملية بين المجتمع والمؤسسات.
- الأمن السيبراني كشرط للتحول الرقمي :أصبح تحقيق الأمن السيبراني ضرورة استراتيجية لضمان نجاح التحول الرقمي في مختلف القطاعات الحكومية والخاصة حول العالم.

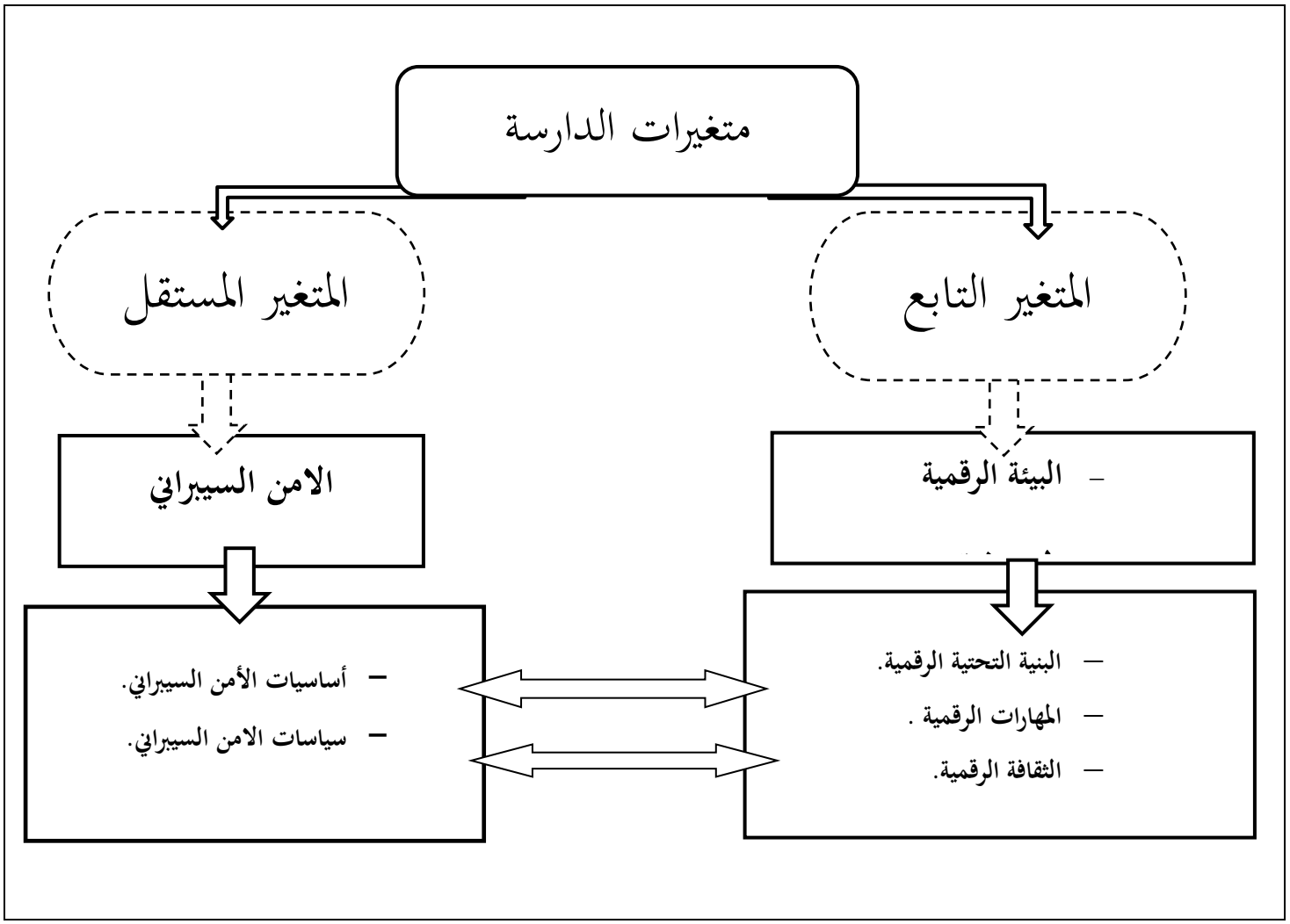
III. نموذج و فرضيات الدراسة

1. نموذج الدراسة:

تم وضع نموذج دراسة في ضوء الدراسات السابقة و البحوث ذات صلة بالموضوع الخاص ببحثنا و يتألف النموذج من متغيرين:

- المتغير الأول: وهو المتغير المستقل و يتمثل في الامن السيبراني.
- المتغير الثاني: وهو المتغير التابع و يتمثل في البيئة الرقمية.

الشكل(01): نموذج يمثل متغيرات الدراسة.



المصدر: من إعداد الطالبة

2. فرضيات الدراسة

وحتى نتمكن من الإجابة عن مختلف التساؤلات المطروحة قمنا بوضع مجموعة من الفرضيات والتي سيتم إما تدعيمها أو نفيها:

- **الفرضية الرئيسة:**
  - **"هناك دور ذو دلالة إحصائية للأمن السيبراني في تحسين البيئة الرقمية في جامعة محمد خيضر بسكرة. عند مستوى الدلالة (0.05)."**

- **الفرضيات الفرعية:**

1. **الفرضية الأولى:** هناك دور ذو دلالة إحصائية للأمن السيبراني في تحسين البنى التحتية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05).
2. **الفرضية الثانية:**. هناك دور ذو دلالة إحصائية بين للأمن السيبراني في تحسين المهارات الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05).
3. **الفرضية الثالثة:** هناك دور ذو دلالة إحصائية بين للأمن السيبراني في تحسين الثقافة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05).

IV. التموضع الأبستمولوجي ومنهجية الدراسة:

1. التموضع الأبستمولوجي:

من أجل إضفاء طابع الشرعية والقبول العلمي على هذا العمل البحثي ونتائجه، تم الاعتماد على كل من النموذج الوضعي الواقعي والنموذج التفسيري، لما يوفره هذان النموذجان من توازن بين الموضوعية والذاتية في تحليل الظواهر الرقمية. ففي سياق دراسة الأمن السيبراني ودوره في تحسين البيئة الرقمية، يسمح النموذج الوضعي بضبط المتغيرات ذات الصلة كأنظمة الحماية، ونقاط الضعف، ومستوى الجاهزية التقنية وقياسها بشكل منهجي، مما يساعد في تقييم فعالية التدابير الأمنية. في المقابل، يتيح النموذج التفسيري فهما أعمق للبعد السلوكي المرتبط باستخدام أدوات الأمن السيبراني، ومدى وعي الأفراد والمؤسسات بمخاطر الفضاء الرقمي، وهو ما يمنح الدراسة بعدا أكثر شمولا لتحليل التفاعل بين التقنية وسلوك المستخدم داخل البيئة الرقمية.

2. منهجية الدراسة:

من اجل دراسة الإشكالية الإجابة على الأسئلة المطرحة والوصل إلى الأهداف المرجوة من الدراسة تم الاعتماد على المنهج الوصفي والمنهج التحليلي حيث أنه تم اعتماد على المنهج الوصفي في جانب النظري قمنا بالتطرق فيه إلى تعرف على ماهية الأمن السيبراني والبيئة الرقمية، والمنهج التحليلي اعتمدنا عليه أكثر في الجانب التطبيقي من خلال تحليل الاستبيان الموزع على أساتذة جامعة محمد خيضر بسكرة

V. تصميم البحث:

يختص هذا العنصر المتعلق بتصميم البحث بتحديد مختلف أبعاد البحث وعناصره والتي تتمثل في:

1. **هدف الدراسة:** تهدف هذه الدراسة إلى:
   - التعرف على أهمية الامن السيبراني ومدى فعاليته في تحسين البيئة الرقمية.
   - كيف يمكن لسياسات الأمن السيبراني في تحسن البنية التحتية الرقمية الجامعية بمحمد خيضر بسكرة.
   - تحليل الدور الذي يلعبه الامن السيبراني في تنمية البيئة الرقمية، وتحسين البيئة الرقمية بجامعة محمد خيضر بسكرة.
2. **نوع الدراسة:** بناء علاقة ارتباط بين الامن السيبراني والبيئة الرقمية.

3. **مدى تدخل الباحث**: تم وصف ودراسة الأحداث كما هي بشكل شبه دقيق وصادق وحيادية التحليل لإنتاج علم موضوعي أي كان التدخل بالحد الأدنى.
4. **التخطيط للدراسة**: الدراسة تناوبية (معلمية ثم تحليلية).
5. **وحدة التحليل**: تتمثل في أساتذة جامعة محمد خيضر بسكرة .
6. **المدى الزمني**: لقد كانت دراسة مقطعية تمت على مرة واحدة حيث تم انجاز الجزء النظري و إعادة صياغته وتعديله كما تم إجراء الجانب التطبيقي وتوزيع استبيان وتحليله وكان هذا خلال بداية شهر افريل 2025.

VI. أهمية الدراسة:

تكتسي هذه الدراسة أهمية بالغة نظرا لتزايد الاعتماد على الأنظمة الرقمية في تسيير مختلف الجوانب الأكاديمية والإدارية داخل الجامعات، وهو ما يجعل من مسألة الأمن السيبراني ركيزة أساسية لضمان حماية المعلومات وضمان استمرارية الخدمات الرقمية. وتبرز أهمية هذا البحث من خلال تركيزه على جامعة محمد خيضر – بسكرة كنموذج للدراسة، بهدف تشخيص واقع البيئة الرقمية في هذه المؤسسة وتحليل التحديات المرتبطة بأمنها السيبراني. كما تسعى الدراسة إلى تقديم رؤية علمية وعملية تساعد على تحسين مستوى الحماية الرقمية، وتعزيز وعي المستخدمين بالمخاطر الإلكترونية المحتملة، الأمر الذي من شأنه أن يسهم في دعم جهود التحول الرقمي الآمن، ويواكب التوجهات الوطنية الرامية إلى تطوير التعليم العالي والبحث العلمي في ظل بيئة رقمية متكاملة وآمنة.

VII. خطة البحث

من من خلال هذه الدراسة، تم تقسيم البحث إلى فصلين رئيسيين، وهما:

– **الفصل النظري**: سنتناول هذا الفصل الجوانب النظرية المتعلقة بموضوع الدراسة، حيث تم تقسيمه إلى ثلاثة مباحث رئيسية: سيتناول المبحث الأول ماهية الأمن السيبراني ومفاهيمه الأساسية، أما المبحث الثاني سنتطرق إلى ماهية البيئة الرقمية، بينما سنخصص المبحث الثالث أهمية الأمن السيبراني في دعم وتطوير البيئة الرقمية.

– **الفصل التطبيقي**: وهو الجانب الميداني من الدراسة، حيث سنحلل فيه دراسة حالة لجامعة محمد خيضر – بسكرة، من خلال توزيع استبيان على مجموعة من أساتذة الجامعة في المبحث الأول سنقدم تعريف عام بالجامعة التي أجريت فيه الدراسة، بينما سنخصص المبحثان الثاني والثالث لتحليل نتائج الاستبيان واختبار الفرضيات المطروحة، باستخدام أدوات وأساليب إحصائية مناسبة.

الفـــــــصل الأول

عموميات حول الامن السيبراني والبيئة الرقمية

تمهيد

في عصرٍ تتسارع فيه وتيرة التكنولوجيا وتتعمق فيه استخدامات الإنترنت، أصبحت التقنية ركيزة أساسية في جميع تفاصيل حياتنا اليومية. ومع هذا التحول، غدت البيئة الرقمية الفضاء الجديد الذي نمارس فيه أعمالنا ونعتمد عليه بشكل متزايد في شتى مجالات الحياة وبموازاة هذا الاعتماد المتزايد، تبرز الحاجة الملحة لحماية المعلومات والبيانات من التهديدات المتصاعدة، وهنا يظهر الأمن السيبراني كخط الدفاع الأول، فهو يشكل الدرع الذي يحمي هذه البيانات من التسريب أو التلاعب، ويضم مجموعة من الإجراءات والتقنيات الهادفة إلى تأمين الأنظمة والشبكات من الهجمات الإلكترونية، وفي ظل تنامي هذه الهجمات وتنوع أساليبها، لم يعد الأمن السيبراني ترفا، بل ضرورة لا غنى عنها لتعزيز الثقة في البيئة الرقمية وبناء مجتمع رقمي آمن ومستقر.

يمثل الأمن السيبراني منظومة متكاملة من السياسات والتقنيات المصممة لضمان حماية البيانات واستمرارية الأنظمة دون اختراق أو عبث فالهجمات السيبرانية اليوم لم تعد مجرد حوادث فردية، بل باتت أدوات تستخدم في الحروب الاقتصادية والمعلوماتية ولهذا، فإن إنشاء بيئة رقمية آمنة لم يعد خيارا، بل ضرورة تفرضها تحديات العصر فالأمن السيبراني لا يحمي الأنظمة فحسب، بل يعزز أيضا الثقة في مسار التحول الرقمي، ويفتح آفاقا واسعة نحو مستقبل أكثر ذكاء وأمانا، وعليه لتعمق اكثر في الموضوع تم التطرق في هذا الفصل الى " عموميات حول الامن السيبراني والبيئة الرقمية " وقد تم تقسيمه الى ثلاث مباحث هي:

- **المبحث الأول: ماهية الامن السيبراني.**
- **المبحث الثاني: ماهية البيئة الرقمية.**
- **المبحث الثالث: التهديدات الامنية السيبرانية في البيئة الرقمية.**

المبحث الأول: ماهية الامن السيبراني.

يشكل الأمن السيبراني أحد الركائز الأساسية في حماية البنية التحتية الرقمية في ظل التطور التقني المتسارع اذ يقوم بتأمين الأنظمة والشبكات من الهجمات السيبرانية التي تهدد سرية البيانات وسلامتها وتوافرها.

المطلب الأول: مفهوم الامن السيبراني.

يشكل الأمن السيبراني أحد الركائز الأساسية في حماية البنية التحتية الرقمية في ظل التطور التقني المتسارع اذ يقوم بتأمين الأنظمة والشبكات من الهجمات السيبرانية ونظرًا لازدياد الاعتماد على البيئة الرقمية، تزداد الحاجة إلى تعزيز آليات الحماية لضمان استمرارية الأداء والتصدي للمخاطر الحديثة.

الفرع الأول: لمحة تاريخية عن المن السيبراني.

بظهور استخدام الكمبيوتر وربطه بالشبكة في الستينيات إلى السبعينيات من القرن الماضي، ظهرت المعالجة الأولى الجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وشكل هذا الموضوع التساؤل فيما إذا كانت هذه الجرائم مجرد حالة عابرة أو ظاهرة اجرامية مستجدة، وبقيت محصورة في إطار السلوك اللا أخلاقي دون النطاق القانوني ومع توسع الدراسات تدريجياً وخلال السبعينيات بدأ الحديث عنها كظاهرة جديدة وفي الثمانينيات ظهر نوع جديد من الجرائم السيبرانية ارتبط بعمليات اقتحام نظم الحاسوب عن بعد، ونشر الفيروسات عبر شبكات الكمبيوتر الذي سبب تدمير الملفات والبرامج، حينها شاع اصطلاح (الهاكرز) المعبر عن مقتحمي النظم، وبقي الحديث دائماً عن دوافع هذه الجرائم محصوراً في اختراق أمن المعلومات وإظهار التفوق التقني من قبل مرتكبي هذه الأفعال الذين لم يتعدوا فئة صغار السن العباقرة في هذا المجال، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف الفاعلين وتحديد طوائفهم ولاسيما بعد تحول الجريمة من مجرد مغامرة إلى أفعال تستهدف التجسس والاستيلاء على البيانات الاقتصادية والاجتماعية والسياسية والعسكرية وشهدت فترة التسعينيات تطوراً هائلاً في مجال الجرائم التقنية وتغيراً في نطاقها وبفعل ما أحدثته شبكة الإنترنت من تسهيل العمليات دخول الأنظمة واقتحام شبكات المعلومات حينما أصبحت مواقع الإنترنت التسويقية النشطة أكثر عرضة للهجمات التي ظهرت بسببها أنماط جديدة من الجرائم، مثل تعطيل النظام التقني ومنعه من القيام بعمله المعتاد الذي يتسبب بالقطاع النظام عن الخدمة لساعات، فتنتج عنه خسائر مالية بالملايين، وقد توسعت جرائم نشر الفيروسات عبر شبكة الإنترنت لما تسهله من وصول إلى ملايين المستخدمين في الوقت نفسه، ليفتح الباب على مصراعيه لمختلف الأفعال غير السوية المتطورة بتطور التقنية، وقد سجلت عبر هذه المراحل مجموعة من القضايا، تلتها الكثير من الحوادث وجرائم المعلوماتية المتعلقة بالأمن السيبراني. (العوادي، 2016، صفحة 4)

وبهذا شهد الأمن السيبراني تطورًا تدريجيًا عبر العقود، مدفوعًا بالتقدم التكنولوجي وظهور التهديدات الرقمية ومنه يمكن التطرق الى أهم المراحل التي أدت الى ظهور الامن السيبراني كالاتي : (maryville university, 2024)

أولا: **مرحلة الستينيات والسبعينيات:** بدأت فكرة أمن الحواسيب بالظهور في الستينيات والسبعينيات، حيث بدأ الباحثون في تطوير مفاهيم أساسية لحماية البيانات أثناء نقلها عبر الشبكات.

أ. في **1965** طرح العالم الويلزي دونالد ديفيز مفهوم "تبديل الحزم(Packet Switching) "، وهو أسلوب لنقل البيانات عبر تقسيمها إلى حزم صغيرة تسلك طرقًا مختلفة للوصول إلى وجهتها، هذا المفهوم أسس للبنية الأساسية للإنترنت، وساهم في تقليل فرص التنصت والتجسس على البيانات.

ب. وفي **1969** تم إنشاء شبكة**ARPANET** من قبل وزارة الدفاع الأمريكية ، والتي تعد أول شبكة ناجحة لتبادل المعلومات بين الحواسيب. هذه الشبكة شكلت النواة الأولى لشبكة الإنترنت الحالية، وفتحت الباب لظهور تحديات جديدة تتعلق بأمن البيانات.

ج. وفي **1971** تم إنشاء أول فيروس حاسوبي باسم **CREEPER**، وهو برنامج ذاتي الانتشار صُمم لإصابة حواسيب PDP-10من شركةDEC ، حيث يعرض رسالة تقول:

"I'M THE CREEPER: CATCH ME IF YOU CAN" وسرعان ما تم تطوير برنامج مضاد له باسم **REAPER**، وهو أول برنامج مضاد فيروسات.

د. وفي **1976** قدم كل من **ويتفيلد ديفي** و**مارتن هيلمان** بروتوكولًا ثوريًا يتيح للطرفين تبادل مفتاح سري عبر قناة غير آمنة. كان هذا تطورًا كبيرًا في مجال التشفير، ويمثل أساس العديد من أنظمة الحماية الرقمية المستخدمة اليوم.

وهذا العرض يوضح النشأة الأولية للأمن السيبراني، حيث بدأت الأفكار تتبلور حول كيفية تأمين المعلومات الرقمية، وهو ما مهد الطريق أمام تطوير تقنيات أكثر تطورًا في العقود التالية.

ثانيا: مرحلة الثمانينيات: بداية عصر مضادات الفيروسات وظهور التهديدات الرقمية: مع تزايد استخدام الحواسيب، بدأت الفيروسات في الظهور، مما استدعى تطوير أدوات للحماية منها. (maryville university, 2024)

أ. في **1983** قام مجموعة من القراصنة تُعرف باسم "414 "كباختراق شبكة**ARPANET** ، ما أبرز مدى هشاشة الشبكات الرقمية في ذلك الوقت، ودفع المؤسسات إلى التفكير الجاد في تعزيز حماية أنظمتها.

ب. وفي **1987** تم تطوير أول برنامج مضاد فيروسات تجاري من قبل شركة .**McAfee Associates**

ج. اما في **1988** أطلق **روبرت تابان موريس** برنامجًا تجريبيًا **Morris Worm** انتشر بطريقة غير متوقعة عبر الإنترنت، مما تسبب في إبطاء الشبكات.

د. مرحلة التسعينيات: صعود الجريمة الإلكترونية وتحديد المعايير ومع انتشار الإنترنت عالميًا، بدأت الهجمات الإلكترونية تتخذ طابعًا أكثر تنظيمًا واحترافية.

هـ. حيث في عام **1991** ظهرت فيروسات المتعددة الأشكال(Polymorphic) قادرة على تغيير شكلها لتفادي الكشف، ما شكل تحديًا جديدًا أمام برامج الحماية التقليدية.

و. في**1995** تم اعتماد معيار تشفير DES كأول محاولة جادة لحماية المعلومات المرسلة إلكترونيًا، وهو حجر الأساس للمعايير التشفيرية الحديثة.

ز. في **1999** انتشر الفيروس **ميليسا**(**Melissa**) بسرعة فائقة عبر البريد الإلكتروني، مُسببًا أضرارًا مالية تجاوزت 80 مليون دولار، ودفع الشركات نحو تحسين أنظمة الأمن لديها.

ثالثا: مرحلة الألفينات: الهجمات السيبرانية والامتثال التنظيمي شهد هذا العقد موجة من الهجمات الكبرى، مما دفع الحكومات والمنظمات إلى تبني لوائح ومعايير أمنية صارمة. (maryville university, 2024)

أ. في **2000** انتشر فيروس "(**ILOVEYOU**) "عالميًا عبر رسائل البريد الإلكتروني، مُسببًا أضرارًا بمليارات الدولارات، وكان من الأسباب المباشرة لتعزيز الوعي الأمني في البريد الإلكتروني.

ب. وفي **2001** استغلت دودة كود ريد(**Code Red**) ثغرة في خوادم مايكروسوفت، مما أحدث اضطرابات كبيرة على الإنترنت.

ج. في عام **2003 ضربت** دودة**SQL Slammer** قواعد البيانات واستهدفت نقاط ضعف محددة في Microsoft SQL Server، ما أبرز أهمية أمن قواعد البيانات.

د. وفي **2006** تشريعات **HIPAA** و**PCI–DSS** فرضت هذه اللوائح على القطاعات الصحية والمالية اعتماد إجراءات أمنية قوية لحماية المعلومات الحساسة، وشكلت منعطفًا مهمًا في مجال الامتثال الأمني.

هـ. وفي العقد **2010**: ظهور الأمن السحابي والتهديدات برعاية الدول مع انتقال الكثير من البيانات إلى الحوسبة السحابية، برزت الحاجة إلى استراتيجيات جديدة للحماية.

و. في**2010** فيروس **Stuxnet**استهدف هذا الفيروس أنظمة التحكم الصناعية، ويُعتقد أنه كان جزءًا من هجوم سيبراني منظم بين دول، مما فتح الباب أمام حقبة جديدة من الحرب السيبرانية.

ز. **2013** اختراق بيانات شركة **Target** أدى إلى تسريب معلومات 40 مليون بطاقة ائتمان، ما دفع متاجر التجزئة إلى تبني أنظمة أمنية متقدمة.

ح. وفي **2017** اجتاحت هجمات **WannaCry** و**NotPetya** العالم وأدت إلى خسائر بمليارات الدولارات، وأظهرت أهمية التحديث المستمر للأنظمة الأمنية.

ط. في العقد **2020**: يتسارع تطور الأمن السيبراني بوتيرة غير مسبوقة بفضل التكنولوجيا الحديثة الذكاء الاصطناعي والحوسبة الكمومية.

ي. وفي سنة **2022** أظهر إطلاق **ChatGPT** كيف يمكن استخدام الذكاء الاصطناعي في اكتشاف التهديدات والرد عليها بشكل أكثر فعالية.

ك. في**2023** تم تطوير خوارزميات مقاومة للحوسبة الكمومية سعيت هذه الخوارزميات لمواجهة تهديدات الحواسيب الكمومية التي قد تكسر أساليب التشفير التقليدية. (maryville university, 2024)

يظهر الأمن السيبراني تطورا مستمرا الى يومنا هذا فتاريخ المعركة بين المهاجمين والمدافعين في تطور دائم، ومع دخول تقنيات مثل الذكاء الاصطناعي والتشفير إلى ساحة المعركة، فإن التعاون والابتكار والتدريب المستمر هي الأسلحة الأهم لضمان مستقبل رقمي آمن.

الفرع الثاني: تعريف الامن السيبراني.

رغم تنوع وتعدد التعريفات المرتبطة بالأمن السيبراني، إلا أن معظمها يتمحور حول مفاهيم متقاربة تُعنى بحماية الأنظمة الرقمية والمعلومات الحساسة من التهديدات السيبرانية. وقد قدّم كل مفكر أو باحث تعريفًا للأمن السيبراني من زاويته الخاصة، وفيما يلي نستعرض بعضًا من أبرز هذه التعريفات التي ساهمت في تشكيل الفهم العام للأمن السيبراني:

إن أساس نشأة كلمة السيبرانية cybernetic ارتبطت باللغة اليونانية والذي يعني التوجيه والسيطرة ومشتقة من كلمة (Kybernetes)أي الشخص الذي يدير دفة السفينة، إذ تستخدم مجازاً للمتحكم (governor) وبذلك بإمكاننا القول أن السيبرانية هي التحكم عن بعد، فهي عندما تأتي مع كلمة أخرى تعني التحكم بها أو إدارتها كما في الأمن السيبراني، أما الأمن فهو نقيض الخوف أي بمعنى السلامة والأمن مصدر الفعل أمن أمناً وأماناً وأمنة أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال أمن من الشر أي سلم منه في إشارة إلى غياب ما يهدد القيم النادرة. (جيجان، 2021، صفحة 35)

نقصد بالأمن السيبراني مجموع الإجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأخرى للمحافظة على سرية المعلومات الالكترونية، ومنع والاختراقات الفيروسية من اجل ضمان وصولها للمعلومات الحاسوبية إلى الجهات المختصة، وفي الوقت المناسب وضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء، خصوصاً بعد الثورة الهائلة في عالم الاتصالات والتداولات الالكترونية شكل هكذا نوع من الامن هاجس استراتيجي للقوى العالمية والمتمثلة بالولايات المتحدة والصين وروسيا فتدور اليوم حرب الالكترونية بين هذه القوى من اجل الاختراق المعلومات والتأثير على اسعار البورصة والعملات. (العلي، 2017، صفحة 224)

كما عرفت وزارة الدفاع الأمريكية "البنتاغون" الأمن السيبراني بأنه جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها المادية والالكترونية من مختلف الجرائم والهجمات التخريب, التجسس الحوادث . (غيدان و الربيعي، 2020، صفحة 188)

و من بين من عرف الأمن السيبراني Edward Amors ، الذي قدم الأمن السيبراني بأنه: الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات ومنها الوسائل المستخدمة في مواجهة القرصنة و كشف الفيروسات، حيث جزم بالجدارة المطلقة لأجهزة الأمن السيبراني في ردع الجريمة المعلوماتية، إلا أن الوسائل المسخرة لحماية المعلوماتية والأمن السيبراني ليس بالضرورة أنها تقوم دائما بردع الجرائم الالكترونية، وإنما قد تعمل على الحد منها والحماية من وقوعها، وأيضا Kemmerer . A Richard الذي يرى أنه : عبارة عن وسائل دفاعية من شأنها كشف و إحباط المحاولات التي يقوم بها القراصنة و يبدو أنه قدم تعريفا مختصرا و لم يفصل في هوية القراصنة و أنواع مرتكبي الهجمات السيبرانية. (بن برغوث، 2023، صفحة 447)

في تعريف اخر ينص الأمن السيبراني على 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 ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك. (هوساوي، 2020، صفحة 41)

بالنسبة للمشرع الجزائري فعرف الأمن السيبراني بانه يمثل مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. (بوازدية، 2021، الصفحات 13-14)

بناء على ما ورد في التعاريف السابقة، يمكن الاعتماد على تعريف شامل ومتكامل للأمن السيبراني، كما يلي: الأمن السيبراني هو مجموعة من السياسات والإجراءات والتقنيات المصممة لحماية الأنظمة الرقمية، والشبكات، والأجهزة، والبيانات من التهديدات السيبرانية، كالهجمات الإلكترونية، والاختراقات، والبرمجيات الخبيثة، والتجسس الإلكتروني. يهدف الأمن السيبراني إلى ضمان سرية المعلومات وسلامتها وتوافرها، والحد من المخاطر الرقمية التي قد تؤثر على الأفراد، المؤسسات، والدول. ويُعد أحد الأركان الأساسية في البنية التحتية للأمن القومي والاقتصادي في ظل تزايد الاعتماد العالمي على الفضاء الرقمي.

الفرع الثالث: مبادئ الامن السيبراني.

استنادا إلى توجيهات الخبراء الإقليميين والأطر الدولية والإقليمية بشأن الأمن السيبراني، فقد حددت جمعية الإنترنت ISOC المبادئ الأساسية التالية لتأمين شبكة الإنترنت : (بن جدو، 2022، صفحة 303)

أ. **الوعي**: يتعين على جميع الجهات المعنية في كل من القطاعين العام والخاص فهم المخاطر التي تهدد أمنها، ومدى تأثير تلك المخاطر عليها وعلى الآخرين في النظام البيئي الخاص بالبنية التحتية لشبكة الإنترنت .

ب. **المسؤولية**: يجب على جميع الجهات المعنية تحمل مسؤولية مواجهة المخاطر الأمنية في إطار أدوارها ومؤسساتها، مع الأخذ في الاعتبار للآثار المترتبة على اتخاذ إجراء ما أو التقاعس عن تنفيذه

ج. **التعاون**: يجب إشراك جميع الجهات المعنية، بما في ذلك الأطراف المعنية خارج الحدود في حوار مستمر حول الأمن السيبراني المواجهة التهديدات الجديدة والمستمرة مواجهة فعالة.

كما ان هناك ثلاثة معايير أساسية اتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار إليها بمثلث أو ثلاثي CIA وهي : (بن جدو، 2022، صفحة 304)

أ. **السرية**: ويقصد بها عدم كشف المعلومات لغير أطرافها بما يوفر الخصوصية والسرية للمعلومات المتداولة على الفضاء الرقمي .

ب. **الأمانة**: وتعني عدم التلاعب بالمعلومات أو حذفها أو تعديلها بحيث يضمن المستخدم دقة نقل ما يريد من معلومات دون تدخل في أثناء النقل أو التخزين أو المعالجة.

ج. **التوافر**: فهو استمرار توفر المعلومة للشخص أو الجهة التي يسمح لها المستخدم بالاطلاع عليها عند الحاجة.

تبرز هذه المبادئ والمعايير الدور الحيوي للوعي والمسؤولية والتعاون في تعزيز الأمن السيبراني، إلى جانب الحفاظ على سرية المعلومات وسلامتها وتوفرها، بما يشكل أساسا لضمان الثقة في البيئة الرقمية المتنامية.

المطلب الثاني: أهمية ومهام بالأمن السيبراني.

في ظل التوسع الهائل في استخدام التقنيات الحديثة والاعتماد المتزايد على الفضاء الرقمي في مختلف مجالات الحياة، برز الأمن السيبراني كحجر أساس لضمان استمرارية الأنظمة وحماية المعلومات، فلم يعد الأمن السيبراني مجرد إجراء تقني، بل أصبح ضرورة استراتيجية تفرضها طبيعة المخاطر المتنامية. ومن هنا تبرز أهمية الأمن السيبراني ومهامه المتعددة التي تهدف إلى تعزيز الحماية، الكشف عن التهديدات، والاستجابة الفعالة لها.

الفرع الأول: أهمية و أهداف الامن السيبراني.

مع التحول الرقمي المتسارع واعتماد المجتمعات الحديثة على التكنولوجيا في مختلف القطاعات، أضحى الأمن السيبراني عنصرًا محوريًا لحماية الأفراد والمؤسسات من المخاطر الإلكترونية. وتزايدت الحاجة إلى وضع استراتيجيات فعّالة تضمن سلامة المعلومات وسرية المعاملات الرقمية. وانطلاقًا من أهمية الدور الذي يلعبه الأمن السيبراني، برزت مجموعة من الأهداف والمهام التي تسعى إلى تحقيق بيئة رقمية أكثر أمانًا واستقرارًا.

أولا: **أهمية الامن السيبراني.**

يظهر الأمن السيبراني أهمية متزايدة في العصر الرقمي، إذ يعد حجر الأساس لحماية البيانات وضمان استمرارية الخدمات. كما يعزز الثقة في البيئة الرقمية من خلال تقليل التهديدات والمخاطر الإلكترونية حيث تتمثل أهمية الأمن السيبراني فيما يلي: (السمحان، 2020، صفحة 12)

أ. **الحفاظ على المعلومات وسلامتها وتجانسها:** يتمثل ذلك في منع أي محاولة غير مصرح بها للتلاعب بالبيانات أو تعديلها أو إفسادها، بما يضمن بقاء المعلومات صحيحة وموثوقة ومتسقة.

ب. **تحقيق وفرة البيانات وجاهزيتها عند الحاجة:** يضمن الأمن السيبراني بقاء المعلومات متاحة للمستخدمين المعنيين في الوقت المناسب، مما يدعم سير العمل بسلاسة ويمنع تعطيل الخدمات الحيوية.

ج. **حماية الأجهزة والشبكات من الاختراقات:** يعمل الأمن السيبراني بمثابة درع واقٍ يحمي أنظمة الحواسيب والشبكات من التهديدات والهجمات الخبيثة، مما يساهم في صون المعلومات وحماية البنية التحتية الرقمية.

د. **استكشاف نقاط الضعف والثغرات ومعالجتها:** من خلال التدقيق الأمني واختبار الاختراق، يمكن اكتشاف الثغرات الأمنية في الأنظمة والشبكات والعمل على إصلاحها قبل أن يستغلها المهاجمون.

هـ. **استخدام أدوات المصادر المفتوحة وتطويرها:** يمثل استغلال أدوات المصادر المفتوحة جانبًا مهمًا لتعزيز مبادئ الأمن السيبراني، حيث توفر هذه الأدوات حلولاً فعّالة ومبتكرة لمواجهة التهديدات الإلكترونية وتطوير دفاعات مرنة ومحدثة.

و. **توفير بيئة عمل آمنة أثناء التعامل عبر الشبكة العنكبوتية:** يسهم الأمن السيبراني في إنشاء بيئات رقمية موثوقة، ما يمنح المستخدمين القدرة على أداء أعمالهم عبر الإنترنت دون الخوف من التعرض للقرصنة أو سرقة البيانات.

تبرز أهمية الأمن السيبراني اليوم كضرورة حيوية في ظل الاعتماد المتزايد على التقنيات الرقمية في مختلف جوانب الحياة. فمع تعاظم التهديدات الإلكترونية، أصبح تأمين البيانات والأنظمة أولوية قصوى لضمان استمرارية الأعمال، وحماية الأفراد والمؤسسات

من المخاطر السيبرانية، وهو ما يتطلب منظومة متكاملة تجمع بين الوقاية والاستجابة والتحديث المستمر للأدوات والبنى التحتية الرقمية.

ثانيا: **أهداف الامن السيبراني**.

يهدف الأمن السيبراني أولًا وأخيرًا إلى حماية الأنظمة الحاسوبية من أي وصول غير مشروع، ومنع العبث بالمعلومات أثناء مراحل التخزين أو المعالجة أو النقل، كما يسعى إلى توفير الحماية ضد أي محاولات لتعطيل الخدمات المقدمة للمستخدمين الشرعيين، بما يضمن استمرارية الأداء واستقرار العمليات الرقمية. وتتمثل الأهداف الأساسية للأمن السيبراني فيما يلي: (حميدي و طايلب، 2022، الصفحات 8-9)

أ. **تحسين مستوى حماية المعلومات**: ضمان سلامة البيانات وصحتها من خلال وضع آليات متطورة للحماية، بما يضمن استمرارية تدفق المعلومات وتشغيل الأنظمة بشكل موثوق وآمن.

ب. **ضمان انسيابية آمنة للمعلومات**: تأمين انتقال البيانات والملفات عبر الشبكات بصورة مشروعة، مع التأكد من أن جميع العمليات تتم بطريقة مصرح بها ومرخصة وفقًا للمعايير الأمنية المعتمدة.

ج. **استرداد البيانات المسربة بأسرع وقت ممكن**: العمل على استرجاع البيانات المخترقة أو المتسربة فور حدوث أي خرق أمني، وتقليل الآثار السلبية المحتملة على الأنظمة والمستخدمين، وذلك عبر خطط استجابة واستعادة مدروسة ومؤمّنة.

وانطلاقًا من ذلك، فإن هدف الأمن السيبراني يتمثل في القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة، والاستجابة لها والتعافي منها، وبالتالي التحرر من المخاطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات، أو نتيجة إساءة استخدامها.

ويتطلب الأمن السيبراني حماية الشبكات وأجهزة الحاسوب، والبرمجيات، والبيانات من الهجمات أو الأضرار أو محاولات الوصول غير المصرح به، وبعبارة أخرى، فإنه لا يعني أكثر من حماية البيانات وصونها، ونظرًا لأهمية الأمن السيبراني في واقع مجتمعات اليوم، فقد جعلته العديد من الدول في صدارة أولوياتها، خاصةً بعد بروز مظاهر الحروب الإلكترونية بين بعض القوى الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حقبة جديدة من الحروب، هي الحروب الإلكترونية. (بن مرزوق و حرشاوي، 2017، صفحة 67)

الفرع الثاني: مهام الامن السيبراني.

ويضطلع الأمن السيبراني بمهام عدة ومتنوعة أهمها: (طواهير، 2023، صفحة 282)

أولا: **حماية المستخدم وضمان أمن الأجهزة الإلكترونية**: وذلك عبر بروتوكولات خاصة منها تشفير البريد الإلكتروني والملفات والبيانات المهمة الأخرى ما يسهم ليس في حماية المعلومات أثناء النقل فقط، بل في حمايتها من الضياع أو السرقة أيضا.

ثانيا: **حماية أنظمة أجهزة الكمبيوتر من الفيروسات**: التي تؤدي إلى مشكلات خطرة أحيانا.

ثالثا: **الحد من الجرائم الإلكترونية التي تشهد تزايدا كبيرا**: ولا سيما مع التطور التكنولوجي المتسارع، إلى جانب حماية المعلومات والبيانات الشخصية الحساسة من الاختراق والسرقة، وحماية المؤسسات والشركات من هجمات البرمجيات الخبيثة التي تهدف إلى الاحتيال والتصيد إضافة إلى منع وقوع محاولات الابتزاز.

رابعا: **منع استخدام المعلومات على نحو غير قانوني**: والحيلولة دون إلحاق الأذى والضرر بالأفراد والكيانات.

خامسا: **المحافظة على سلامة المجتمع وأمنه بحماية معلوماته الخاصة**: في القطاعات كلها من دون استثناء، ولا سيما تلك المتعلقة بخدمات الرعاية الصحية والتعليمية والمالية وخدمات الطاقة وغيرها. وثمة أهمية خاصة للأمن السيبراني في الاقتصاد، وخاصة القطاع المالي إذ يحمي المصارف والشركات من التهديدات التي قد تلحق الضرر بها وبعملائها؛ ما يؤدي إلى فقدان الثقة بها ولذا فالأمن السيبراني ركيزة أساسية لمنع الخسائر المالية التي قد تصيب المصارف والشركات وغيرها من المؤسسات المالية نتيجة تعرض بيانات عملائها لهجمات بهدف السرقة أو التلاعب .

سادسا: **الإسهام في تعزيز الأمن القومي**: مع تزايد اعتماد الدول على "الرقمنة" في مجالات محورية مثل القطاع العسكري، سواء فيما يخص المعلومات أو الأسلحة التي أصبح بعضها موجها، بل يحتاج استخدامه إلى برمجيات خاصة، ومن ثم فإن الأمن السيبراني ضروري لحماية الأمن القومي للدول، بل أصبح جزءا لا يتجزأ منه ليس لدوره في حماية المعلومات والأسرار العسكرية فحسب، وإنما حماية مختلف القطاعات الحيوية من الهجمات الإلكترونية، وحفظ بياناتها، وضمان استمراريتها وتطورها.

المطلب الثالث: فواعل وابعاد الامن السيبراني.

أصبح الأمن السيبراني مجالًا معقدًا يشمل أطرافًا متعددة وأبعادًا متنوعة، لم يعد يقتصر الأمر على حماية الأنظمة التقنية فقط، بل امتد ليشمل أبعادًا سياسية واقتصادية واجتماعية، تتداخل فيها مسؤوليات الحكومات، والمؤسسات، والأفراد، ومن هنا تبرز أهمية فهم الفواعل المؤثرة في الأمن السيبراني، وكذلك استيعاب أبعاده المختلفة، لضمان بناء منظومة دفاعية شاملة وقادرة على التصدي لمختلف التهديدات الرقمية.

الفرع الأول: فواعل الامن السيبراني.

يحدد جوزيف ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة السيبرانية: (العمارات، 2022، الصفحات 25-26)

أولا: **الدول**: والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها، فالدولة هي الفاعل المحوري بامتياز في هذا العالم الافتراضي لما لها من مكانة على أساس التفوق التكنولوجي والمؤهلات التي ترشحها لتبني هذه المكانة.

ثانيا: الفواعل غير الدولاتية: ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية، وتشمل هذه الفواعل ما يلي:

أ. **الشركات المتعددة الجنسيات**: تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على الدول، فخوادم شركات مثل: جوجل Google وفيسبوك Facebook ، ومايكروسوفت Microsoft ، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

ب. **المنظمات الإجرامية**: تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال كما توجد سوق سوداء على الإنترنت المظلم "Dark internet لتجارة المخدرات والأسلحة، والاتجار بالبشر.

ج. **الجماعات الإرهابية**: تعد من أبرز الفواعل الدولية، خاصة بعد أحداث ١١ سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة، وتدريب المجندين الجدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول.

ثالثا: **الأفراد**: أصبح الفرد بفضل الفضاء السيبراني فاعلاً مؤثراً في العلاقات الدولية، ومن أبرز النماذج ظاهرة الويكي ليكس "Wikileaks" الذي نجح في نشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها ما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.

الفرع الثاني: ابعاد الامن السيبراني.

يمتد مفهوم الأمن السيبراني ليشمل الأنظمة العسكرية والاقتصادية والاجتماعية والسياسية والإنسانية، حيث يسعى إلى حماية مختلف القطاعات من التهديدات الإلكترونية المتنوعة. ويعتمد الأمن السيبراني على منظومة متكاملة تعمل على تعزيز كافة أبعاد الحماية الرقمية وضمان استمراريتها. ومن أبرز الأبعاد الخاصة بالأمن السيبراني التي تعد ركائز أساسية لتحقيق هذا الهدف نجد:

أولا: **البعد العسكري**: ويهدف إلى الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية مما يتيح تبادل وتدفق المعلومات والأوامر، وإنها فكرة لإنشاء ونشر شبكة للإنترنت والأهداف البعيدة، ولكنها أيضا نقطة ضعف، خاصةً إذا كانت غير آمنة، ويمكن أن يؤدي تدمير قواعد البيانات العسكرية أو المساومة عليها إلى تعطيل الاتصالات بين وحدات القيادة والوحدات العسكرية، فضلاً عن إمكانية التحكم وفقدان السيطرة على بعض الأسلحة مثل الطائرات بدون طيار والصواريخ الموجهة والأقمار الصناعية. (دحماني، 2023، صفحة 603)

ثانيا: **البعد الاقتصادي** : نظرًا لاستخدام أجهزة الكمبيوتر لتشغيل الصناعات وتنميتها ودفع الاقتصاد، ستصبح الإنترنت أساس التجارة والتمويل والمعاملات المالية، وكلها مرتبطة ببعضها البعض من خلال شبكات الكمبيوتر لتحقيق الأمن السيبراني خصوصا ما تعلق بالقطاع المالي. (دحماني، 2023، صفحة 603)

ثالثا: **البعد الاجتماعي**: من الضروري تعميم المفهوم الصحيح والسليم للأمن إلى كل المشتركين في الشبكة الدولية للمعلومات، إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن إذا ما صيغت بطريقة واضحة وعرفت ونفذت بذكاء، ولذلك يعتبر تنظيم الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسؤول من الضرورة بمكان، بحيث تغطي التحديات والمخاطر، وتدابير الأمن والوقائية والرادعة لأجل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن، وينبغي التشديد على واجب الأمن والمسؤولية الفردية والتدابير الرادعة، وكذلك التداعيات المحتملة في إطار القانون الجنائي التي تترتب على عدم احترام الالتزامات التي يوجبها الأمن، وبصورة أكثر عمومية، فإن من الضروري توفير التثقيف والتدريب على تكنولوجيات المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة، إذ يجب للثقافة الأمنية أن تغرس داخل ثقافة تكنولوجيا المعلومات، كما ينبغي جعل الشبكة الدولية

للمعلومات مشاعا مفتوحا للجميع بحيث يمكن لجميع المتعاملين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية زائدة ويحتاج الأمر إلى بلورة مدونة أخلاقيات الأمن، تكون مقبولة ومحترمة من جانب جميع العاملين في الفضاء السيبراني. (بارة، 2017، صفحة 262)

رابعا: **الأبعاد السياسية**: يتمثل البعد السياسي للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية، التي تعني حقها وواجبها في السعي إلى تحقيق رفاه شعبها في وقت تؤثر موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان الفرد أن يتحول إلى لاعب أساسي في اللعبة السياسية كما أصبح بإمكانه الاطلاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها، وبالمقابل لا يتوانى العاملون في الشأن السياسي من الاستفادة مما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة من الأفراد والترويج لسياساتهم في العالم، ومدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات والمبادئ والمواقف التي تروج لها. (عطية، 2019، الصفحات 106-105)

خامسا: **البعد القانوني** : يترتب على النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، نتائج قانونية، وموجبات تستدعي اهتماما خاص، لحل النزاعات التي يمكن أن تنشأ عنها. وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات. فظهرت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، وتوسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات على الأنترنت، والحق في حماية ملكية البرامج المعلوماتية. كما ظهرت موجبات جديدة، ذات انعكاسات اقتصادية مثل: موجب الاحتفاظ ببيانات الاتصالات، وموجب الابلاغ عن مخالفات وجرائم خاصة بالمحتوى، كل هذه التغيرات والتحولات تستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة، إن على مستوى الحقوق، أو على مستوى البيئات والعمليات. (بارة، 2017، صفحة 263).

يمكن تحديد متطلبات الأمن السيبراني فيما يتعلق بأنواع الهجمات التي تتم ملاحظتها في الوقت المناسب قد توجد نقاط الهجمات أو نقاط الضعف في أحد مكونات الشبكة المتعددة الشبكة في جوهرها هي مزيج من مكونين رئيسيين هما مكونات البرامج والأجهزة تعمل مكونات البرامج للوظائف الداخلية والخارجية على حد سواء، وتشكل مكونات الأجهزة الهيكل المادي للشبكة، فيما يلي بعض أنواع الأمان السيبراني المعروفة: (Humayun Bakht، 2020، الصفحات 8-9)

أولا: **أمان التطبيق**: أمان التطبيق هو الإجراء لحماية الرموز داخل التطبيق من الضياع أو السرقة تضمن هذه الإجراءات أيضا سلامة التطبيق بمجرد نشر التطبيقات نظرًا للأمان الإلكتروني، يأخذ أمان التطبيق في الاعتبار حماية الأنظمة والشبكة من القرصنة أو التطفل المماثل على الرغم من ذلك ، فهي مشكلة صعبة بسبب وجود ثغرات داخل البرنامج أو التطبيق والتي يمكن استخدامها من قبل مخترق لغزو الخصوصية أو سرقة بيانات فرد أو مؤسسة.

ثانيا: **أمن الشبكة**: شبكة يختلط المنشأ على كل من الأجهزة والبرمجيات حيث يعمل البرنامج على مستوى التطبيق والأجهزة يؤسس البنية الأساسية المادية، الأمن السيبراني يحمي الأنظمة التي ترتبط على الانترنت في حين أمن الشبكات أمنة الصورة البنية التحتية للشبكة من خلالها يتم تشكيل شبكة ويمكن جعل الاتصال عبر الإنترنت باستخدام نفس الشبكة

ثالثا: **الأمن السحابي:** توفر الحوسبة السحابية خدمات معالجة المعلومات عبر الإنترنت من خلال السحابة النظام، الجهاز لحفظ، مشاركة البيانات منذ يتم تأمين البيانات والتعامل مع أكثر من بعد الإنترنت يجعل من سحابة بيئة مفتوحة لحساب الأمن السيبراني التهديد الصورة يمكن تعريف الأمن السحابي على أنه الإجراءات والسياسات المعتمدة لتوفير الأمن السيبراني.

رابعا: **أمن إنترنت الأشياء(IoT)** : يشير إنترنت الأشياء إلى اتصال الأجهزة الممكنة للإنترنت ببعضها البعض لاسلكيا يتعامل أمان إنترنت الأشياء (IoT) مع أمان الأجهزة الممكنة للإنترنت ضد أي تهديد محتمل للأمن السيبراني.

المبحث الثاني: ماهية البيئة الرقمية.

أدى التحول الرقمي العميق الذي يشهده العالم في العصر التكنولوجي إلى نشوء بيئة رقمية متكاملة، باتت تمثل حاضنة خصبة للإبداع والابتكار في مختلف المجالات، لا سيما تلك المرتبطة بالتكنولوجيا. فقد أصبح بإمكان الباحث أو المبدع، بفضل هذه البيئة، أن ينفّذ معظم مراحل العمل البحثي أو الإبداعي بشكل فردي، باستخدام أدوات رقمية متطورة. ولم يعد الحصول على المعرفة والتخصصات المتقدمة حكرًا على المؤسسات التقليدية، بل أضحى متاحًا عبر المنصات الرقمية التي توفر سهولة الوصول، وسرعة التفاعل، وتكامل الموارد. وهكذا، أصبحت البيئة الرقمية رافعة حقيقية للمواهب والكفاءات، وساهمت في تسريع وتيرة الابتكار في مجتمعات المعرفة

المطلب الأول: مفهوم البيئة الرقمية.

في ظل التحولات التكنولوجية المتسارعة، برزت البيئة الرقمية كإطار جديد يُعيد تشكيل طرق التواصل والعمل وتبادل المعلومات. فقد أصبحت هذه البيئة جزءًا لا يتجزأ من مختلف المجالات، سواء التعليمية أو الاقتصادية أو الاجتماعية.

الفرع الأول: تعريف البيئة الرقمية.

نظرًا لصعوبة تحديد هذا المصطلح، الذي يعود أساسًا إلى صعوبة التعامل معه، حاول بعض الباحثين والفقهاء تقديم تعريفات متعددة للبيئة الرقمية والتي سنتطرق لبعضها تاليا:

يمكن تحديد مصطلح البيئة الرقمية في أنه منطلق من أن الوسائل التكنولوجية الحديثة تعبر عن أبرز معالم التحول من البيئة القديمة إلى بيئة رقمية جديدة، و إحلال وسائل الاتصال الرقمية محل الاتصالات الشخصية و الاتصال الوسيطي محل الاتصال المواجهي في شؤون الحياة الاجتماعية للناس من أسهلها لأكثرها تعقيدا، من أجل فهم البيئة الرقمية و محاولة التكيف معها و مع انعكاساتها و أبعادها المتعددة والتي تفترض بدورها تغيّرا في الذهنيات التقليدية و السلوكيات و طرق التعامل مع الآخرين، و مواكبة كل جديد في مجال التقنية و دمجه في الحياة الاجتماعي. (نوي، 2016، صفحة 62)

فقد عرفها أحد المفكرين بأنها: "تلك البيئة التي يتم من خلالها تبادل المعلومات بشكل رقمي عبر وسائل اتصال جديدة تتيح الوصول المباشر إلى أكبر قاعدة من المعلومات، سواء بغرض التجارة أو التعليم أو الخدمات". (لواعر، 2023، صفحة 15)

والبيئة الرقمية هي عبارة عن كل متكامل من مجموعة من المفاهيم الحديثة مثل: نظم البحث بالاتصال المباشر، النشر الالكتروني، قواعد البيانات على الأقراص المدمجة، الفهارس الألية، شبكات المعلومات فائقة السرعة متمثلة في شبكة الانترنيت. (هادف، 2022، صفحة 244)

وفي تعريف اخر البيئة الرقمية: هي أجهزة أو برامج تستخدم تطبيق او خدمة ما تعمل وفق نظام تشغيل وتنسيق البرامج التي تستخدم مجموعة من التعليمات لمعالج معين ارضيات عن بعد قائمة على تكنولوجيات الويب وتتكون من عرض تقني وتجاري متماسك من اجل النفاذ الى عالم من الخدمات البعيدة التفاعلية او غير التفاعلية والتي يمكن بثها او توفيرها على الخط والتي يمكن ان تخضع اما للدفع او تكون مجانية والوصول اليها اما محدود او غير محدود ويعتمد العرض على تطوير مجتمع من المستخدمين. (بليج و قوراري ، 2024، صفحة 487)

كما تعني البيئة الرقمية هي بيئة يتمكن فيها المستفيد من الوصول إلى المعلومات من أي مكان ومن خلال أي جهاز حاسوب، دون أن تكون المعلومات والمراجع فيها منظمة بشكل تقليدي. ولذلك، يحتاج الباحث في هذه البيئة إلى استخدام استراتيجيات وأساليب محددة لاسترجاع المراجع والمصادر التي يبحث عنها. ومن هنا، نلاحظ أن بيئة الإنترنت لا تتطلب من الباحث سوى توفر شبكة اتصال وجهاز حاسوب للولوج إليها. وعليه، يمكن اعتبار شبكة الإنترنت تجسيدًا فعليًا لمفهوم البيئة الرقمية. (بن راشد و بلحاح، 2022، صفحة 797)

من هذه التعاريف يمكن تقديم تعريفا شاملا للبيئة الرقمية بانها: منظومة متكاملة ناتجة عن التحول العميق الذي أحدثته الوسائل التكنولوجية الحديثة في مختلف مناحي الحياة، حيث انتقلت المجتمعات من نمط الاتصالات التقليدية إلى تفاعلات رقمية متطورة تدار عبر أجهزة وأنظمة وبرمجيات متصلة بشبكات عالية السرعة، وتمثل هذه البيئة فضاء افتراضيا يتيح تبادل المعلومات والمعارف بشكل مباشر وآني، ويعتمد على مجموعة من التطبيقات والخدمات التي يمكن الوصول إليها من أي مكان وفي أي وقت، سواء لأغراض تجارية، تعليمية، بحثية أو خدمية، كما تتسم بمرونتها وانفتاحها، مما يتطلب من الأفراد تطوير مهارات جديدة للتعامل مع كم هائل من البيانات غير المنظمة، باستخدام استراتيجيات وتقنيات رقمية متقدمة. وتؤدي هذه البيئة إلى إعادة تشكيل السلوكيات، الذهنيات، وأساليب التفاعل الاجتماعي بما يتلاءم مع متطلبات العصر الرقمي المتسارع.

الفرع الثاني: أسباب التحول من البيئة التقليدية الى البيئة الرقمية.

لقد أسهمت البيئة الرقمية في إحداث نقلة نوعية داخل الفضاء المعرفي، فكانت بمثابة تحول جذري عن البيئة التقليدية التي اعتمدت على الوثائق الورقية والأنظمة اليدوية في تداول المعلومات، هذا التحول لم يكن اعتباطيًا، بل جاء نتيجة حتمية لتطور التكنولوجيا الحديثة، وازدياد الحاجة إلى حلول ذكية وسريعة لمواجهة الكم الهائل من الوثائق والمعلومات التي باتت المؤسسات تعاني من صعوبة في تنظيمها وتخزينها بالطريقة التقليدية. ولعلّ أبرز العوامل التي ساعدت على الانتقال من البيئة التقليدية إلى البيئة الرقمية هو الاتجاه الواسع نحو رقمنة نظم المعلومات داخل المؤسسات، إذ عمدت هذه الأخيرة إلى تحويل أرشيفاتها ووثائقها إلى وسائط رقمية مرنة تُسهم في تسريع وتسهيل الوصول إلى المعلومة عند الحاجة. (لواعر، 2023، صفحة 16)

وفي هذا السياق، أصبحت سرعة الحصول على المعلومات وتقديمها للمستخدمين من المؤشرات الأساسية لتقييم مدى نجاح المؤسسات وفعاليتها، ما جعل الرقمنة أداة لا غنى عنها لتحسين الأداء وضمان الاستجابة السريعة لمتطلبات العمل. كما دفعت الحاجة إلى إمكانية الوصول إلى الوثائق عن بُعد إلى رقمنتها وإتاحتها عبر الإنترنت، مما خفف الضغط على الإدارات المركزية، وحقق لامركزية في تداول المعلومات ومرونة في استخدامها.

من جهة أخرى، أدت البيئة الرقمية إلى بروز ظواهر جديدة في الفضاء التواصلي، كان أبرزها انتشار شبكات التواصل الاجتماعي، التي أصبحت تلعب دورًا محوريًا كمصدر للمعلومة ومجال لنشر الإنتاجات الفكرية والإبداعية. فبفضل هذه المنصات الرقمية، أتيحت الفرصة للمؤلفين والمبدعين لنشر أعمالهم الأدبية والفنية على نطاق واسع، خارج القيود التقليدية لدور النشر الورقية. كما ساهم هذا التحول في ظهور نماذج اقتصادية جديدة، كعمليات البيع والشراء الإلكترونية، التي تعكس وجود بيئة استثمارية رقمية واعدة، تُمكن المبدعين من تسويق أعمالهم الصناعية والفكرية على نطاق عالمي، دون حواجز زمانية أو مكانية، وبأدوات تفاعلية متطورة. (لواعر، 2023، صفحة 16)

ويمكن ان تعد المجالات الخمسة التالية من أهم الأسباب الدافعة نحو التحول الى البيئة الرقمية والتي يمكن ذكرها في: (ضيف الله، 2017/2016، صفحة 84)

أ. **تطورات الإنترنت المتلاحقة وتفاعلاتها في البيئة الرقمية:** أدى التطور السريع والمستمر للإنترنت وتفاعلها مع أدوات البيئة الرقمية إلى ظهور نماذج أعمال جديدة تتسم بانخفاض التكاليف وسهولة التشغيل، مما مكّن من إنشاء أنشطة اقتصادية جديدة تعتمد على الإدارة الإلكترونية، مثل الأعمال الإلكترونية والتجارة الإلكترونية والحكومات الإلكترونية. هذا التطور أدى إلى تراجع تدريجي في الاعتماد على نماذج الأعمال التقليدية التي كانت تفرض قيودًا مكانية وزمنية على العمليات.

ب. **ظهور وتطور اقتصاد المعرفة في ظل البيئة الرقمية:** برز مفهوم اقتصاد المعرفة كنتيجة طبيعية لتحول المعلومات إلى مورد اقتصادي أساسي، حيث أصبحت المعرفة أصولًا استراتيجية تنتج من خلالها منتجات وخدمات جديدة. بمعنى آخر، لم تعد القيمة الاقتصادية تُقاس فقط بالسلع المادية، بل أصبحت المعلومات والمعرفة أدوات إنتاجية رئيسية تدفع بعجلة الابتكار والتنمية.

ج. **النمو في الاقتصاد المرتبط عالميًا بفضل البيئة الرقمية:** أدى ترابط الأسواق العالمية عبر الإنترنت وما تتيحه البيئة الرقمية من شبكات اتصال وتوزيع إلى نشوء اقتصاد عالمي متداخل يُشار إليه بمصطلح "العولمة". ويظهر ذلك من خلال القدرة على إدارة الأسواق الإلكترونية العالمية، وخلق منافسة على نطاق عالمي، بالإضافة إلى إمكانية تشكيل فرق عمل موزعة دوليًا تتواصل وتعمل بكفاءة عالية بفضل البنية الرقمية العابرة للحدود.

د. **التحولات في نماذج الأعمال نتيجة البيئة الرقمية:** أصبحت البيئة الرقمية عاملاً رئيسيًا في إعادة تشكيل الطريقة التي تُدار بها المؤسسات، حيث بات بالإمكان إنجاز الأعمال عبر حدود المؤسسة، سواء الإدارية أو الجغرافية، بنفس الفاعلية تقريبًا التي يتم بها تنفيذ الأعمال داخلها، وهذا التحول يشير إلى أن مفهوم المؤسسة التقليدية لم يعد يحدّ من نطاق الأنشطة، بل أصبح بالإمكان توسيع العمل عبر منصات رقمية متصلة.

هـ. **ظهور مفهوم "الشركة الرقمية" في بيئة الأعمال:** مع تزايد الاعتماد على البيئة الرقمية، برزت "الشركة الرقمية" كمفهوم حديث يصف المؤسسات التي تُدار معظم عملياتها وعلاقاتها الحيوية إلكترونيًا. ويشمل ذلك التفاعل مع الزبائن، والموردين، والعاملين داخل المنظمة، حيث تتم تهيئة كافة العمليات والوظائف بما يتوافق مع البنية الرقمية. ويرتبط ذلك بإعادة تصميم تنظيمي شامل يهدف إلى تحقيق الكفاءة والمرونة من خلال التكيف الكامل مع البيئة الرقمية.

المطلب الثاني: خصائص وأهمية البيئة الرقمية.

لم تعد البيئة الرقمية مجرد خيار تقني، بل أصبحت واقعاً يفرض نفسه على مختلف مناحي الحياة، من التعليم إلى الاقتصاد، ومن الإدارة إلى التفاعل الاجتماعي. ولفهم هذا التحول وفوائده المتعددة، من الضروري الوقوف على خصائص البيئة الرقمية التي تميزها عن البيئات التقليدية، وتوضيح أهميتها في تعزيز الكفاءة، وتيسير الوصول إلى المعرفة، ودعم الابتكار في جميع المجالات.

الفرع الأول: خصائص البيئة الرقمية.

برزت البيئة الرقمية كإطار جديد لتنظيم المعلومات وتبادلها حيث تتميز بخصائص فريدة تسهم في إعادة تشكيل طرق التفاعل والعمل، مما يستدعي فهما دقيقا لهذه السمات لتوظيفها بشكل فعال في مختلف المجالات. وعليه فيمكن ذكر اهم خصائص للبيئة الرقمية فيمايلي: (صالح، 2020، الصفحات 244-246)

1. **تقليص الوقت** :تسهم البيئة الرقمية في تقليص الزمن اللازم لإنجاز المهام، حيث يمكن تنفيذ العمليات والوصول إلى المعلومات بسرعة فائقة، مما يعزز الكفاءة والإنتاجية.
2. **تقليص المكان**: تتيح الوسائط الرقمية تخزين كميات هائلة من البيانات والمعلومات في مساحات افتراضية، مما يقلل الحاجة إلى المساحات الفيزيائية الكبيرة.
3. **اقتسام المهام الفكرية مع الآلة**: تمكن البيئة الرقمية من توزيع بعض المهام الفكرية بين الإنسان والآلة، من خلال استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي، مما يعزز من فعالية العمل.
4. **قابلية التحويل** :تتميز البيئة الرقمية بمرونتها في تحويل المعلومات من صيغة إلى أخرى، مثل تحويل النصوص إلى صوت أو العكس، مما يسهل الوصول إلى المحتوى بمختلف الأشكال.
5. **اللاجماهرية** :تسمح البيئة الرقمية بتوجيه الرسائل والمحتوى إلى فئات محددة من الجمهور وتعني إمكانية توجيه الرسالة الاتصالية إلى فرد واحد أو جماعة معنية بدل توجيهها بالضرورة إلى جماهير ضخمة، وهذا يعني إمكانية التحكم فيها حيث تصل مباشرة من المنتج إلى المستهلك، كما أنها تسمح بالجمع بين الأنواع المختلفة للاتصالات، سواء من شخص واحد إلى شخص واحد، أو من جهة واحدة إلى مجموعات ، أو من مجموعة إلى مجموعة
6. **الشيوع والانتشار** :تتميز البيئة الرقمية بقدرتها على الانتشار الواسع، حيث يمكن للمحتوى الرقمي الوصول إلى جمهور عالمي دون قيود جغرافية.
7. **العالمية** :تعمل البيئة الرقمية في نطاق عالمي، مما يتيح تبادل المعلومات والخدمات عبر الحدود بسهولة، ويعزز من التعاون الدولي.
8. **الوفرة** :توفر البيئة الرقمية إمكانية الوصول إلى المعلومات والخدمات على مدار الساعة، مما يضمن توفرها في أي وقت يحتاجه المستخدمون. (عباس و علك، 2014، صفحة 64)
9. **سهولة الوصول** :تُسهل البيئة الرقمية الوصول إلى المعلومات والخدمات من أي مكان، باستخدام أجهزة متصلة بالإنترنت، مما يعزز من مرونة الاستخدام.
10. **الاعتمادية**: توفر البيئة الرقمية أنظمة موثوقة تضمن دقة المعلومات وسرعة الوصول إليها، مما يعزز من ثقة المستخدمين في استخدامها.

11 **القابلية للتوسع**: تتميز البيئة الرقمية بقدرتها على التوسع لمواكبة النمو في حجم البيانات وعدد المستخدمين، مما يضمن استمرارية الخدمات دون انقطاع. (عباس و علك، 2014، صفحة 64)

12 **خاصية الحداثة**: حيث أن ما يميز بيئة الأنترنت قدرتها العالية على تحديث معلوماتها، وتعتبر الحداثة صفة ملازمة المعلومات هذه البيئة التي تتميز بالتجدد المتسارع لمعلوماتها، على عكس البيئة التقليدية التي تتصف ببطء شديد في عملية التحيين " وتحديث المعلومات والذي يستغرق وقتا طويلا، قد يكون كافيا لتقادم هذه المعلومات في ظل الإنفجار المعرفي والتسارع الكبير في إنتاج المعلومات (لحواطي، 2014، صفحة 52)

13 **تزايد الاهتمام بمسألة الأمن**: إن تلاشي الحدود المكانية وسيادة الفضاء المفتوح، إلى جانب غياب المركزية وعدم وجود جهة تتحكم بمفاصل السلطة داخل الفضاء المعلوماتي، جعل المجتمع أكثر عرضة للتهديدات المعلوماتية التي قد تمسّ كثيرًا من مرتكزاته الحيوية ويضاف إلى ذلك وجود ثغرات في أمن المعلومات نتيجة لتنامي خبرات المستخدمين، وتقادم التقنيات الرقمية بسرعة كبيرة، مما يُسهم في تعميق المخاطر المحتملة للتهديدات أو الهجمات المعلوماتية. (ومان، 2016، صفحة 88)

تعد هذه الخصائص من السمات البارزة للبيئة الرقمية، التي تسهم في تحسين الكفاءة وتسهيل الوصول إلى المعلومات والخدمات في العصر الحديث.

الفرع الثاني: أهمية البيئة الرقمية.

تعد البيئة الرقمية محركًا رئيسيًا للتحول في مختلف مجالات الحياة، حيث تتجاوز كونها مجرد أدوات تقنية لتصبح بنية تحتية استراتيجية تؤثر على النظم الاقتصادية والاجتماعية والثقافية .يُعزى ذلك إلى قدرتها على تحسين الكفاءة وتسهيل اتخاذ القرارات وتعزيز التفاعل بين الأفراد والمؤسسات .فيما يلي توضيح لأهميتها من عدة جوانب: (النوري و جمعة، 2015، صفحة 97)

أ. **الأهمية الاستراتيجية** :تعتبر البيئة الرقمية عنصرًا حاسمًا في تحقيق التنمية المستدامة، حيث تُمكّن الدول من تعزيز الحوكمة الإلكترونية وتطوير البنية التحتية الرقمية، مما يسهم في تحسين الخدمات العامة وتعزيز الشفافية والمساءلة.

ب. **الأهمية الاقتصادية** :تسهم البيئة الرقمية في تعزيز الاقتصاد الرقمي من خلال دعم التجارة الإلكترونية وتسهيل المعاملات المالية، مما يؤدي إلى زيادة الإنتاجية وتوسيع الأسواق وخلق فرص عمل جديدة .كما تُعتبر مصدرًا للقيمة المضافة من خلال الابتكار وتطوير المنتجات والخدمات الرقمية.

ج. **الأهمية الاجتماعية** :تعزز البيئة الرقمية التفاعل الاجتماعي وتُسهم في نشر المعرفة والثقافة من خلال وسائل التواصل الاجتماعي والمنصات التعليمية الرقمية .كما تُوفر فرصًا للتعلم المستمر وتطوير المهارات، مما يسهم في بناء مجتمع معرفي متقدم.

د. **الأهمية الإنتاجية** :تساعد البيئة الرقمية في تحسين العمليات الإدارية والإنتاجية من خلال الأتمتة وتحليل البيانات، مما يُسهم في رفع كفاءة المؤسسات وتسهيل اتخاذ القرارات الاستراتيجية .كما تُوفر أدوات للتخطيط ومراقبة الأداء، مما يُعزز القدرة التنافسية للمؤسسات في السوق.

في ضوء هذه الأبعاد، يتضح أن البيئة الرقمية تعد ركيزة أساسية لتحقيق التقدم والتنمية في العصر الحديث، مما يستدعي تبني استراتيجيات فعالة للاستفادة من إمكاناتها في مختلف القطاعات كما تسهِم البيئة الرقمية في تحقيق أقصى درجات الإنتاجية عندما

تستخدم كأداة مساعدة للتفكير والتحليل، وليس فقط كوسيلة لتحسين الكفاءة الإدارية حيث تتجلى هذه القيمة من خلال عدة عوامل، منها: (شكر، 2011، الصفحات 14-16)

أ. **التوقيت المناسب** :توفير المعلومات في الوقت الذي تحتاج فيه يعزز من سرعة ودقة اتخاذ القرارات.

ب. **الخصوصية** :ضمان حماية البيانات والمعلومات الحساسة يعزز من الثقة في النظام الرقمي.

ج. **إمكانية التخزين** :القدرة على تخزين كميات ضخمة من المعلومات لفترات طويلة تسهل من عملية الوصول إليها عند الحاجة.

د. **الأمان** :توفير بيئة رقمية آمنة يقلل من مخاطر الاختراقات والتلاعب بالمعلومات.

هـ. **درجة الثقة** :ضمان دقة وصحة المعلومات يُعزِّز من موثوقية النظام الرقمي.

حيث تتميز البيئة الرقمية بالعمل على نشر مجتمع معلوماتي ، ومن ثم تشجيع الحكومة الإلكترونية، البنوك، الصريفة و الإدارة ا الإلكترونية، ، ويحتاج كل ذلك إلى التطور المستمر في مؤشر مجتمع المعلومات والمعرفة عن طريق زيادة أعداد الحواسيب الإلكترونية، واستخداماتها في المعاملات، واستخدام البرمجيات الجاهزة والمفصلة في إدارة الموارد البشرية والأنشطة التعليمية والتدريبية. (بوخباش و يحة، 2019، صفحة 03)

المطلب الثالث: مكونات البيئة الرقمية وأبعادها.

لفهم التحول المتسارع الذي يشهده العالم نحو البيئة الرقمية بشكل شامل، من الضروري التعمق في مكونات البيئة الرقمية وأبعادها، حيث تشكل هذه العناصر الأساس الذي يُبنى عليه المجتمع الرقمي الحديث

الفرع الأول: مكونات البيئة الرقمية.

تعد البيئة الرقمية نظاما متكاملا يتكون من عدة مكونات أساسية تمكن من إنتاج وتبادل واستخدام المعلومات بشكل فعال وتتضمن هذه المكونات: (زازل، 2024، صفحة 58)

1. **المعلومة على الشكل الرقمي** :تشير إلى تحويل البيانات والمحتوى إلى صيغ رقمية قابلة للمعالجة والتخزين والنقل عبر الوسائط الإلكترونية ويشمل ذلك النصوص، الصور، الفيديوهات، والبيانات الأخرى التي تخزن وتعالج باستخدام الحواسيب والأنظمة الرقمية.
2. **التكنولوجيات الحديثة لنقل المعلومات والاتصال** :تشمل البنية التحتية الرقمية مثل شبكات الإنترنت، الاتصالات اللاسلكية، الألياف البصرية، وأنظمة الحوسبة السحابية تعد هذه التقنيات ضرورية لنقل البيانات بسرعة وكفاءة بين المستخدمين والأجهزة المختلف.
3. **الوسائل التقنية المستعملة من قبل المستعمل للوصول إلى المعلومة** :تتضمن الأجهزة والبرمجيات التي يستخدمها الأفراد للوصول إلى المعلومات الرقمية، مثل الحواسيب، الهواتف الذكية، التطبيقات، والمتصفحاتو تعتبر هذه الوسائل الجسر بين المستخدمين والمحتوى الرقمي. (السيد و حوتيه، 2023، صفحة 18)

تتكامل هذه المكونات لتشكيل بيئة رقمية تمكِّن من الوصول السريع والفعال إلى المعلومات، وتسهل التفاعل والتواصل في العصر الرقمي.

الفرع الثاني: أبعاد البيئة الرقمية.

تعد البيئة الرقمية إطارًا متكاملاً يشمل مجموعة من الأبعاد التي تتفاعل فيما بينها لتشكيل فضاء رقمي فعال ومترابط، فهي تمثل الجوانب المختلفة التي تؤثر وتتأثر بالبيئة الرقمية، حيث تتمثل هذه الابعاد في: (نجم، 2022، الصفحات 56-70)

أولا: **الثقافة الرقمية:** يتضمن هذا البعد الهام العلاقة بين الثقافة ووسائل الاتصال الرقمية كما يعتبر مفهوم الثقافة من إحدى الأفكار التي ساعدت العالم على تحقيق الكثير من جوانب التقدم والتطور الاجتماعي، ويرجع ذلك بصفة خاصة إلى ما يحتوي عليه هذا المفهوم من عناصر داخلية، بمعنى أن كل البشر لديهم ثقافتهم الخاصة، ولا يوجد مجتمعاً إنسانياً يخلو من الثقافة، وانطلاقاً من أن الثقافة مكتسبة، ينقلها الأفراد جيلاً بعد جيل عن طريق مؤسسات اجتماعية بدءً من الأسرة، من خلال التفاعل الاجتماعي في صورة الاتصال وعن طريق مؤسسات اجتماعية إلى جانب المجتمع الرقمي تعتبر مجالات اجتماعية لنقل الثقافة الرقمية، حيث في نظرية وسائل الاتصالات والإعلام وكذا تقنيات المعلومات، فإن العالم بأكمله تحول من الثقافة المطبوعة السائدة في القرن19 نحو الثقافة الإلكترونية في القرن 20 وصولاً إلى الثقافة الرقمية في القرن 21 والتي وثقت بشكل جيد، وظهرت بشكل واسع وسريع بسبب شبكات الحواسيب والاستعمالات المتعددة للبرمجيات وشبكة المعلومات العالمية .

كما أننا نجد أن مفهوم الثقافة الرقمية من المفاهيم الحديثة في العلوم الاجتماعية، فهو يشير إلى المجال الذي يرتبط به المجال الرقمي وتعني التمكن من مجال معين أو امتلاك الفرد للسلوكيات المعرفية التي يستطيع من خلالها التفاعل مع هذا المجال، وذلك يدل على أن جوهر الثقافة الرقمية يكمن في تمكن أفراد المجتمع من استخدام التطبيقات الرقمية نظراً لأهميتها في إنجاز أعمالهم الوظيفية والشخصية، وأصبحت هذه الممارسات أكثر من موضة أو تجميل للسلوك الإنساني، وأصبح الواحد والصفر هما البنية الأساسية لعصر الثقافة الرقمية، ويشير مصطلح الثقافة الرقمية إلى مدى انخراط الفرد أو المستخدم وانسجامه مع مجتمع رقمي ما، بالإضافة إلى القوانين والأنظمة المفروضة في مجتمع رقمي ما واستشعار الرقابة الذاتية لتحقيق الترابط بين أفراد المجتمع، بحيث يكون المستخدم في هذا النوع من المجتمعات المستحدثة خاضعاً للعديد من الإجراءات والأنماط والقوانين التي نطلب منه التفاعل بشكل إيجابي مع بيئة فالثقافة الرقمية قد تكون تعبيراً عن مميزات فترة زمنية ما، فالعالم يعيش حالياً مرحلة من التطور التكنولوجي تمتزج فيها ثلاث ثورات هي ثورة المعلومات المتمثلة في الانفجار الضخم في المعرفة، ثورة وسائل الاتصال وتتجسد في تطور تكنولوجيا الاتصال الحديثة

ثانيا: **المهارات الرقمية** : تعتبر المهارات الرقمية من أهم المهارات المرنة التي ينبغي أن تتوفر في الموارد البشرية خصوصاً في ظل المجتمع الرقمي وللحديث عن هذه المهارات الرقمية يجب التعرف على مفهوم المهارة ثم المهارات الرقمية، وعليه فإنه يمكن القول بأن "المهارة" هي: مستوى القابلية والاستعداد والاستطاعة على تطبيق المعرفة بدرجة إتقان تتكافأ مع مستوى المعرفة اللازمة لأداء الوظيفة من ناحية ومع نوع القدرة التي تمثل أحد مكونات الكفاءة الكلية التي لا يمكن أن ننجز الوظيفة إلا بتوافرها ويشير مصطلح المهارات الرقمية إلى الاستخدام الناقد والحاسم لتكنولوجيا المجتمع الرقمي من أجل العمل والترفيه والتعلم والاتصال، وهي مدعومة بالمهارات الأساسية في مجال تكنولوجيا المعلومات والاتصالات، أي استخدام الحواسيب لاسترجاعها والوصول إليها وتخزينها وإنتاجها وتقديمها وتبادل المعلومات، والتواصل والمشاركة في شبكات التعاونية عبر الإنترنت حيث تعددت وجهات النظر حول تحديد المهارات الرقمية، فمنهم من قام بتحديدها فيما يلي:

أ. مهارات في تكنولوجيا المعلومات الرقمية.

ب. مهارات الاتصالات الرقمية.

ج. مهارات تنمية مكونات الشخصية الإنسانية.

د. مهارات إدارة التغيير والتطوير.

هـ. مهارات حل المشكلات

و. مهارات التواصل

ز. مهارات الانشاء

ح. مهارات التعامل عبر الانترنت

ط. مهارات تشغيلية

ثالثا: الشمولية **الرقمية** : تعتبر الشمولية الرقمية من أهم الأبعاد الاستراتيجية لبناء بيئة الرقمي، فهي تعني: العمل على تيسير النفاذ الشامل لكافة القطاعات وفئات المجتمع في المنطقة للاستفادة من الخدمات الرقمية المختلفة لتكنولوجيا المعلومات والاتصالات الرقمية وتحسين جودة هذه الخدمات خاصة في المناطق المعزولة والنائية.

حيث يشير مفهوم الشمولية الرقمية إلى توفير نفاذ متساوي ومشاركة شاملة الجميع الأفراد في تكنولوجيا المعلومات والاتصالات الرقمية بهدف تشجيع استخدام التكنولوجيا للتغلب على الإقصاء المجتمعي تحسين الأداء الاقتصادي، وتعزيز فرص العمل وجودة الحياة وتحقيق مجتمع رقمي شامل ولتحقيق الشمولية الرقمية يجب أن تحتوي على مجموعة من العناصر الأساسية، ويمكن تحديدهم في الآتي:

أ. خدمة إنترنت موثوقة وقوية وبتكلفة ميسورة.

ب. أجهزة مزودة بخدمة الإنترنت والتي تلبي احتياجات المستخدم.

ج. توفير الوصول إلى الدورات التدريبية لمحو الأمية الرقمية.

د. توفير الدعم التقني المناسب.

هـ. توفير تطبيقات ومحتوى عبر الإنترنت هدفها تمكين وتشجيع الاكتفاء الذاتي والمشاركة والتعاون.

و. ينبغي أن تتمتع المناطق الفقيرة والمناطق الريفية قدر الإمكان بالقدرات

ز. الإلكترونية الكافية لتقديم المساعدة إلى المستخدمين في المكتبات أو المؤسسات

ح. التعليمية أو مكاتب البريد أو الادارات العامة

ثالثا: **تكنولوجيا المعلومات والاتصالات**: تعد التكنولوجيا من أكثر الألفاظ شيوعاً واستخداماً في عصرنا حتى من قبل المواطن العادي، فقد اكتسب لفظ التكنولوجيا الكثير من المطاطية حتى أصبح يعني أشياء كثيرة ومختلفة ومتناقضة حسب مستخدم اللفظ فمن الصعب التوصل إلى تعريف موحد للتكنولوجيا يقبل به الجميع، ويرجع ذلك إلى الجوانب اللغوية والتاريخية التي ارتبط بلفظ تكنولوجيا على مر السنين حيث الوضوح أكثر في هذا المجال نجد جنباً إلى جنب لفظ تكنيك ولفظ تكنيك" ولفظ تكنولوجيا، فالأول لفظ قديم والثاني لفظ حديث نسبياً، والتكنيك هو الأسلوب الذي يستخدمه الإنسان في إنجاز عمل أو عملية ما، أما التكنولوجيا بمعناها الأصلي فهي علم الفنون والمهن والتكنولوجيا مصطلح مركب من كلمتين يونانيتين هما "Tekhe ومعناها مهنة

و Logos علم فالتكنولوجيا عملية Process بمعنى أنها كيان يضم أجزاء متشابهة، أما التكنيك فهو نتاج Product العملية التكنولوجية نفسها، الذي ينتج عنها تكنيك وأساليب محددة، وهذا التكنيك أو هذه الأساليب قد تكون خدمة أو سلعة محددة وتغطي تكنولوجيا المعلومات استخدام كل من الحاسبات الإلكترونية ووسائل الاتصال عن بعد وأجهزة التصوير والاستنساخ المصغر في نظم استرجاع المعلومات وفي تقديم خدمات المعلومات وتعرف تكنولوجيا المعلومات على أنها: "التكنولوجيا الإلكترونية والرقمية المتمثلة في استخدام الحاسبات والاتصالات الإلكترونيات المصغرة التي تستخدم في إنتاج وتجميع وتخزين ومعالجة وتناقل وبث نتائج عمليات تحليل وتصنيف واستخلاص المعلومات وتوجيه الإفادة منها من قبل المستفيدين بأيسر السبل مع ضمان السرعة والدقة في النتائج أكثر من استخدام الطرق النمطية والتقليدية ولابد أن تتسم تكنولوجيا المعلومات والاتصالات داخل المؤسسات والمنظمات بالخصائص الآتية :

أ. **القبول** : أي أن تنال وسائل تكنولوجيا المعلومات رضا وقبول كل من العاملين عليها والمستفيدين منها، والاقتناع بانا تعود عليهم بالفائدة.

ب. البساطة تعني سهولة فهم واستخدام تكنولوجيا المعلومات والاستفادة منها.

ج. **الاعتمادية**: يقصد بها درجة الثقة في مخرجاتها والتي تمكن المستخدمين من الاعتماد عليها في اتخاذ القرارات ومواجهة المواقف المختلفة.

د. **المرونة** وتعني قدرة تكنولوجيا المعلومات على الاستجابة على المتغيرات التي قد يطرأ في الظروف والمتغيرات البيئية.

رابعا: **تدفق البيانات والمعلومات**: ويعتبر هذا البعد من أهم الأبعاد التي كان لها دور كبير في بناء المجتمع الرقمي، فقد تعددت التعريفات المرتبطة بمفهوم المعلومات ولكن قبل تناول هذه التعريفات يجب التفريق بين مصطلح "البيانات" ومصطلح "المعلومات"، البيانات "Data" يقصد بها المادة الأولية، وهي المعطيات البكر التي نستخلص منها المعلومات، وهي بنود البطاقة الشخصية، ومادة استيفاء النماذج، وقراءات أجهزة القياس والإشارات التي تنبعث من أجهزة الإرسال وتلتقطها أجهزة الاستقبال، فهي إشارات أو رموز معنوية أو أرقام أو جمل أو عبارات متفق عليها رسمياً لتمثيل الأفراد أو الحوادث، أو المفاهيم، وهي خالية من المعنى لظاهري، ولا قيمة لها بشكلها المحدد وتعتبر المعلومات من أهم مكونات الحياة المعاصرة بل أنها تشكل عنصر التحدي لكل فرد في المجتمع، ومما سبق نجد أن البيئة الرقمية المعاصرة ومؤسساتها العلمية والثقافية والإنتاجية أصبحت تواجه تدفقا هائلا في البيانات والمعلومات وذلك يرجع إلى:

أ. التطورات العلمية والتقنية الحديثة.

ب. تحول إنتاج المعلومات إلى صناعة.

ج. ظهور التخصصات التكنولوجية الجديدة.

د. نمو القوى المنتجة والمستهلكة والمستفيدة من المعلومات.

هـ. تراكم هائل في رصيد المعلومات نظراً لأنها متجددة ولا تتناقص. (نجم، 2022، الصفحات 56-70)

المطلب الرابع: مزايا وتحديات البيئة الرقمية.

من خلال دمج التكنولوجيا في الأنشطة اليومية فقد أصبحت الوسائط الرقمية، مثل الإنترنت والتطبيقات الذكية، أدوات رئيسية في التعليم، والتجارة، والاتصال، مما أدى إلى تغييرات جذرية في أساليب العمل والتفاعل الاجتماعي ومع هذه التحولات، برزت مزايا عديدة للبيئة الرقمية، إلا أنها جاءت أيضًا بتحديات جديدة تتطلب فهما عميقا واستراتيجيات فعالة للتعامل معها.

الفرع الأول: مزايا البيئية الرقمية.

تعد البيئة الرقمية إطارًا شاملاً يجمع بين التقنيات الرقمية والبنى التحتية والموارد البشرية، مما يمكن الأفراد والمؤسسات من التفاعل مع المعلومات والخدمات بشكل فعال، اذ تقدم البيئة الرقمية مزايا متعددة تعزز من جودة الحياة وتسهم في تطوير مختلف القطاعات وهي تتمثل في: (ياسع، 2011، صفحة 27)

أ. **تحسين جودة الحياة** :تسهم الخدمات الرقمية في مجالات التعليم، الطب، التجارة، والاتصالات في تعزيز شعور الأفراد بالحرية، حيث تُقلل من القيود الزمنية والمكانية، مما يُتيح لهم الوصول إلى الخدمات والمعلومات في أي وقت ومن أي مكان.

ب. **تعزيز البحث العلمي** :توفر البيئة الرقمية أدوات ومنصات تُسهل من عملية البحث العلمي، حيث تُتيح الوصول إلى مصادر المعلومات بسرعة وكفاءة، مما يُعزز من جودة الأبحاث ويُسرع من وتيرة الاكتشافات العلمية.

ج. **تنوع الموارد الترفيهية والثقافية** :تُقدم البيئة الرقمية مجموعة واسعة من الموارد في مجالات الترفيه، السفر، والسياحة، بالإضافة إلى المنتديات الإلكترونية التي تُشجع على التفاعل وتبادل الآراء بين الأفراد.

د. **تطوير التجارة الإلكترونية** :أدت الثورة الرقمية إلى نمو التجارة الإلكترونية، حيث أصبح بإمكان المؤسسات التجارية تقديم سلع وخدمات عبر الإنترنت، مما يُحسن من مستوى الخدمة ويُعزز من العلاقات مع العملاء والموردين.

هـ. **تحسين وسائل الإعلام** :تلعب الصحافة الإلكترونية دورًا هامًا في نشر المعلومات والتواصل بين الشعوب، مما يُسهم في تعزيز الوعي والتفاهم الثقافي.

و. **تقليل التكاليف التشغيلية** :تُقلل البيئة الرقمية من الحاجة إلى الاتصالات الشخصية المباشرة، مما يُخفض من تكاليف التنقل والإقامة، ويُسهم في تحقيق تكامل عالمي لأسواق رأس المال.

ز. **تعزيز كفاءة الموارد البشرية** :تُركز البيئة الرقمية على تحسين كفاءة العنصر البشري، من خلال توفير أدوات تُساعد في أداء الأعمال بسرعة وفعالية.

ح. **تسريع تدفق المعلومات** :تُتيح البيئة الرقمية تدفقًا سريعًا وكثيفًا للمعلومات، مما يُمكن الأفراد من تنمية قدراتهم واتخاذ قرارات مستنيرة.

ط. **ابتكار أنماط إنتاجية جديدة** :أدت البيئة الرقمية إلى ظهور أنماط جديدة في الإنتاج والاستهلاك، حيث يُركز الإنتاج على الابتكار والتخصيص بدلاً من التكرار، مما يُعزز من التنافسية والمرونة في السوق.

ي. تقديم آليات تيسر العمل بالمؤسسات كالأعمال المكتبية والبحثية كانت تستدعي وقتا طويلا وأفراد كثر. (السيد و حوتيه، 2023، صفحة 18)

ك. وفرة التصنيع للأجهزة والبرمجيات ، وبروز منتوجات جيدة وانخفاض في الأسعار.

ل. الانفتاح على العالم الخارجي، فيمكن تبادل المعلومات بين جهازين مرتبطين داخل دولة بنفس الطريقة وبدون تغيير بين جهازين يكونان متباعدين وغير موجودين في نفس البلاد ولا حتى في نفس القارة، مما يجعل العالم كما يقال قرية إلكترونية والايجابي جدا هو تحمل نفس التكلفة بين المستعملين . (السيد و حوتيه، 2023، صفحة 18)

الفرع الثاني: تحديات البيئة الرقمية.

رغم ما توفره البيئة الرقمية من مزايا وفرص، فإنها تواجه مجموعة من التحديات التي تؤثر على الأفراد والمجتمعات والدول، ومن أبرز هذه التحديات: (ياسع، 2011، صفحة 28)

أ. **الفجوة الرقمية والمعرفية** :تستمر الفجوة بين الأفراد والدول في الوصول إلى التقنيات الرقمية والمعرفة، مما يؤدي إلى ظهور فئات محرومة من فوائد الثورة الرقمية، ويشار إليهم أحيانًا بـ"فقراء المعلومات."

ب. **الواقع الافتراضي والتلاعب بالمعلومات** :أدخلت البيئة الرقمية مفاهيم جديدة مثل الواقع الافتراضي، مما يتيح للبعض إمكانية التلاعب بالحقائق التاريخية والمعلومات، مما قد يؤثر على فهم الأفراد للتاريخ والواقع.

ج. **التأثير النفسي والاجتماعي** :قضاء فترات طويلة أمام الشاشات والتنقل بين المواقع الإلكترونية قد يؤدي إلى ضغوط نفسية وعصبية، خاصة بين الأطفال والمراهقين، نتيجة التعرض المستمر للمعلومات والانفصال عن الواقع الاجتماعي.

د. **انتهاك الخصوصية** :تُعد اختراقات الخصوصية من أبرز تحديات البيئة الرقمية، حيث يمكن الوصول إلى البيانات الشخصية والحساسة للأفراد والمؤسسات، مما يشكل تهديدًا للأمن الشخصي والمؤسسي.

هـ. **التهديدات الأمنية والجرائم الإلكترونية** :تُعتبر البيئة الرقمية ساحة جديدة للجرائم، مثل الهجمات السيبرانية والاحتيال الإلكتروني، مما يشكل تهديدًا للأمن القومي والمجتمعي.

و. **التأثيرات الصحية** :التعرض المستمر للموجات الكهرومغناطيسية المنبعثة من الأجهزة الرقمية قد يكون له آثار سلبية على الصحة، مثل مشاكل الأعصاب وزيادة مخاطر بعض الأمراض.

ز. **انتهاك حقوق الملكية الفكرية** :سهولة نسخ وتوزيع المحتوى الرقمي تؤدي إلى زيادة حالات انتهاك حقوق المؤلف والناشر، مما يؤثر على الإبداع والابتكار.

ح. **تأثيرات على سوق العمل** :رغم أن البيئة الرقمية توفر فرص عمل جديدة، إلا أنها قد تؤدي أيضا إلى فقدان بعض الوظائف التقليدية، مما يخلق تحديات في التوظيف والتأهيل المهني.

ط. **نشر الأفكار المتطرفة** :تُستخدم بعض المنصات الرقمية لنشر الأفكار المتطرفة والدعوات التحريضية، مما قد يؤدي إلى زعزعة الاستقرار الاجتماعي والسياسي.

المبحث الثالث: التهديدات الامنية السيبرانية في البيئة الرقمية.

تعتمد المجتمعات بشكل متزايد على التكنولوجيا في مختلف جوانب الحياة ومع هذا التوسع، برزت تحديات أمنية جديدة تتطلب اهتماما خاصا.

المطلب الأول: دواعي الاهتمام بالأمن السيبراني في البيئة الرقمية.

رغم أن الأمن السيبراني موجود منذ وجود الحاسوب نفسه، فقد بدأ هذا الموضوع يحظى باهتمام متزايد وغير مسبوق على المستوى العالمي، وذلك بالنظر إلى: (طواهير، 2023، الصفحات 281-282)

أولا: **المخاطر التي تنطوي على التهديد الإلكتروني** على مختلف نواحي الحياة، حيث يمكن أن يتسبب في وقف قطاعات حيوية أو حتى تدميرها.

ثانياً :**تنوع هذه التهديدات المتعلقة بالأمن السيبراني**، حيث تشمل:

أ. **الجرائم الإلكترونية**: التي تشمل قيام أفراد أو مجموعات باستهداف النظم الإلكترونية من أجل مكاسب مادية أو الحصول على فدية مالية أو لخلق اضطراب وخلل فيها، ووفقاً لتقرير صادر عن موقع متخصص في هذا المجال، فإن معدل تكلفة الجرائم الإلكترونية لأي منظمة زادت بنسبة 23% في سنة 2022 وقد تُكلف العالم 10 تريليونات دولار سنوياً في 2025 وفقاً لتقرير آخر.

ب. **الهجمات السيبرانية**: التي تهدف عادة إلى جمع معلومات لدوافع سياسية أو لاستغلالها في تضليل الناخبين مثلاً، كما حصل في الانتخابات الرئاسية في الولايات المتحدة عام 2016، حيث خلصت التحقيقات إلى أن دولة تدخلت إلكترونيا لتأثير توجهات الناخبين، ما ساهم بشكل أو بآخر في فوز أحد المرشحين وخسارة الآخر.

ج. **الإرهاب الإلكتروني**: الذي يعني تقويض النظم الإلكترونية بهدف إحداث الرعب أو الخوف، والتي قد يستخدمها أفراد أو جماعات بأيديولوجية دينية أو سياسية.

باختصار، إن الأمن السيبراني مهم جدا لأنه يحمي أفراد والشركات والمؤسسات من أي تهديد إلكتروني محتمل، فالتطور التكنولوجي ترك كثيراً من الناس والدول عرضة لهجمات إجرامية سيبرانية، فمعادلات الجرائم الإلكترونية تزيد ومن ثمّ فمن دون أمن سيبراني فإن الأفراد والشركات والمؤسسات، وكذلك الدول، قد تخسر المعلومات الحساسة والأموال وحتى السمعة والثقة أما أحدث التهديدات السيبرانية التي يحتاجها الأفراد والمنظمات على حد سواء إلى الحماية منها، فهي البرامج الخبيثة التي تؤثر تأثيراً خطيراً في الحكومة والجمهور والبنية التحتية والشركات في جميع أنحاء العالم، التحايل إذ تُركب كثير من الجرائم باستخدام مواقع معينة وعن طريق تطبيقات مختلفة منها تطبيقات "المواعدة"، وغرف الدردشة، وغير ذلك من التهديدات التي تصعب مواجهتها أحياناً، ولأنّ هذه التهديدات جميعها بالطبع تُحدث تبعات خطرة اقتصادياً واجتماعياً وأمنياً.

المطلب الثاني: تهديدات الامن السيبراني في البيئة الرقمية.

هناك تحديات وتهديدات عديدة تواجه الأمن السيبراني، تمثل أكبر آفة يتعامل معها العالم الرقمي، والتي غالبا ما تتسبب في خسائر فادحة يصعب التعامل معها، ودور الأمن السيبراني هنا ألا يقوم بالدفاع ضد هجماتها فحسب، بل أن يقوم بمنع حدوثها من الأساس اذ يمكن رصد أبرز هذه التحديات والتهديدات وأكثرها شيوعا كالتالي :(الخبيزي، 2023، الصفحات 241-246)

أ. **البرمجيات الخبيثة:** البرامج الخبيثة أو البرامج الضارة هي نوع من البرامج المصممة للوصول غير المصرح به إلى جهاز الكمبيوتر أو إلحاق الضرر به بمعني أنها تتضمن مجموعة من البرامج التي تم إنشاؤها من أجل منح أطراف ثالثة إمكانية الوصول غير المصرح به إلى المعلومات الحساسة أو السماح لها بتعطيل سير العمل العادي للبنية الأساسية بالغة الأهمية تشمل الأمثلة الشائعة للبرمجيات الخبيثة أحصنة طروادة وبرامج التجسس والفيروسات. وبكلمات أخري فإن البرمجيات الخبيثة هي فيروسات متقدمة يتم تصميمها بهدف الالتفاف عن أنظمة الحماية المثبتة على النظام والعمل على إحداث ضرر أو خلل فيها، مما يسمح بالتلاعب أو السيطرة على البيانات الحساسة معتمدة في الأساس على الثغرات التي يمكن استغلالها.

ب. **فيروس الفدية الخبيث:** تشير برامج الفدية الخبيث إلى نموذج عمل ومجموعة واسعة من التقنيات ذات الصلة التي تستخدمها الجهات المسيئة لابتزاز الأموال من الكيانات. ويعد فيروس الفدية الخبيث واحد من أخطر الهجمات الإلكترونية في عالمنا الرقمي الحالي والتي طبقا للإحصائيات العالمية الأخيرة فإن هناك هجوم من نوع الفدية الخبيث تقريبا كل 10 ثواني على الأقل، وفيه يتم حجب كافة البيانات الخاصة بالضحية وتشفيرها، وعدم السماح له بالدخول عليها إلا بعد دفع فدية مالية كبرى، وكلما كانت هذه البيانات سرية وحساسة، كلما أستغل أصحاب هذه الفيروسات الأمر وفرضوا أوامر تعجيزية كبرى، والتي لا يملك فيها الضحية إلا الرضوخ لها في النهاية.

ج. **تصيد البيانات والمعلومات:** هو عملية إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من المصادر الموثوقة والهدف هو سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان ومعلومات تسجيل الدخول بمعني أن تصيد المعلومات عملية يتم من خلالها استغلال قلة الثقافة الإلكترونية للضحية أو عدم انتباه لما يعرض أمامه من معلومات، وجعله يشارك بمحض إرادته معلومات حساسة خاصة ببطاقته الائتمانية أو معلومات سرية لا يجب مشاركتها مع العوام ككلمة السر الخاصة بتسجيل الدخول في المنصات الرقمية أو غير من المواقع. وتعد عملية تصيد المعلومات من أكثر أنواع الهجمات الإلكترونية شيوعًا، حيث بلغت نسبة 80% من نسبة الهجمات التي تتم على الأفراد والمؤسسات، وطبقا لجوجل تم تقدير أكثر من 2.1 مليون موقع مخصص لذلك في عام 2020 م وحده

د. **استغلال البرامج الثنائية أو ما يعرف بهجوم الوسيط:** في الهجوم الوسيط، يحاول طرف خارجي الوصول بشكل غير مصرح به إلى الاتصالات في شبكة أثناء تبادل البيانات تزيد مثل هذه الهجمات من المخاطر الأمنية للمعلومات الحساسة، مثل البيانات المالية ويعد هجوم الوسيط واحد من الأدوات الشائعة المستخدمة في عمليات الهجمات السيبرانية، وفيها يستغل المهاجم لجوء الضحية إلى مصدر تقني ثاني ضعيف الحماية، ويقوم بالدخول إلى النظام من خلاله كاستغلال شبكة الوايفاي والعمل على اختراق النظام الخاص بالأجهزة المشتركة فيها والعمل على تثبيت برامج خبيثة تساعد في السيطرة عليها .

هـ. **التصيد الاحتيالي أو المباشر**: أو ما يعرف بالتصيد بالرمح التصيد الاحتيالي أو هجمات التصيد هو تهديد سيبراني يستخدم تقنيات الهندسة الاجتماعية من أجل خداع المستخدمين للكشف عن معلومات التعريف الشخصية على سبيل المثال، يرسل المهاجمون السيبرانيون رسائل إلكترونية تستدرج المستخدمين للنقر عليها وإدخال بيانات بطاقة الائتمان في صفحة ويب وهمية لإتمام الدفع. يمكن أن تؤدي هجمات التصيد الاحتيالي أيضا إلى تنزيل مرفقات ضارة تثبت برامج ضارة على أجهزة المؤسسة أو الشركة. وفي التصيد الاحتيالي يتم استهداف فرد أو مؤسسة بحد ذاتها، والعمل على دراسة كل أنظمة الدفاع والحماية الخاصة بها بالتفصيل، ثم العمل على اكتشاف الثغرات التي يحتويها النظام وآلية تطويعها لصالح عملية اختراق وسيطرة ممنهجة.

و. **التسلسل المتقدم طويل الأمد**: وفيها يتم اختراق أنظمة الحماية بشكل خفي وتدريجي، بحيث لا يتم اكتشافه إلا بعد مرور فترة زمنية طويلة، والتي من خلالها يكون الضرر قد تم بالفعل وتمت السيطرة الكلية على النظام بنجاح.

ز. **هجمات رفض الخدمة**: وفيها يتم إمطار النظام بوابل من حركات المرور والرسائل والمستخدمين الوهميين، بحيث ينشأ نوع من الضغط على الخوادم وتعطيلها أو التسبب في بطئها، مما يتسبب بوقوع خسائر فادحة ولاسيما إذا كان هذا الهجوم في وقت خاص تتوقع فيه الشركة تحقيق مكاسب كبيرة من إقبال الزائرين عليها وخاصة في وقت المواسم أو التخفيضات أو بعد الإعلان على عروض تنافسية قوية.

ح. **التحايل باستخدام الهندسة الاجتماعية**: الهندسة الاجتماعية ويطلق عليها أحيانا بعلم وفن اختراق العقول، ولقد انتشر هذا المصطلح مع انتشار وسائل التواصل الاجتماعي وتعددها، ويشير التحايل باستخدام الهندسة الاجتماعية إلى مجموعة الأساليب التي يستخدمها المجرمون في الحصول على المعلومات الحساسة، أو اقناع الضحايا بتنفيذ بعض الإجراءات التي تساعد على اختراق أنظمتهم والإضرار بهم، وهناك من عرف التحايل باستخدام الهندسة الاجتماعية بأنها نوع من أنواع الهجوم على السرية، وتنطوي على عملية التلاعب النفسي في أداء الأعمال، أو دفع الضحية للتخلي عن معلومات مهمة بمعني أنها أسلوب يستخدمه الخصوم لاستدراج البعض إلى الكشف عن المعلومات السرية أو الحساسة الخاصة بهم، بقصد الضرر أو طلب مبالغ نقدية . ويعتبر التحاليل باستخدام الهندسة الاجتماعية من أخطر التحديات والتهديدات للأمن السيبراني وأكثرها انتشارا لأنها لا تقتصر على الاتصال عبر شبكة الإنترنت، بل قد تتم من خلال المواقف الحياتية للضحية، ويستغل المهاجمون ما ينشره رواد وسائل التواصل الاجتماعي من معلومات للإيقاع بهم وايذائهم بشكل أو باخر أيضا ترجع خطورة التحايل باستخدام الهندسة الاجتماعية إمكانية دمجه مع أي من التهديدات المذكورة أنفا.

ط. **هجمات البلوكتشين والعملات المشفرة** : تستهدف هجمات البلوكتشين والعملات المشفرة Block chain and crypto currency attacks بيانات الشركات الكبيرة الأمر الذي من شأنه أن يعرض بيانات العملاء فيها والعمليات التجارية التي تقوم بها إلى مخاطر كبيرة وآثار كارثية لا حصر لها

ي. **هجمات الذكاء الاصطناعي**: ببساطة يعرف الذكاء الاصطناعي بأنه عمل برامج حاسب الي قادرة علي محاكاة السلوك الإنساني المتسم بالذكاء وهو أيضا دراسة القدرات الذهنية من خلال استخدام النماذج الحاسوبية ويستخدم منفذي هجمات السيبرانية هجمات الذكاء الاصطناعي كوسيلة للوصول إلى المعلومات والبيانات الخاصة بالشركات والتي تكون ذات قيمة عالية من أجل تحقيق مكاسب مادية على حساب هذه الشركات.

ك. **الهجمات الداخلية:** تعد الهجمات الداخلية من التحديات الكبيرة التي تواجه الأمن السيبراني لاسيما أنها لهجمات الداخلية تعد الهجمات الداخلية من التحديات الكبيرة التي تواجه الأمن السيبراني لا سيما أنها عمليات تخريب تصدر من داخل الشركة أو المؤسسة ذاتها ومن قبل أشخاص يعملون فيها بهدف تسريب بعض البيانات لشركات منافسة أخرى. وتؤدي الهجمات الداخلية إلى إلحاق خسائر مالية كبيرة في الشركة التي تتعرض لها

ل. **هجمات إنترنت الأشياء:** يقصد بإنترنت الأشياء إلى مجموعة من الأجهزة المتصلة والوسائل التكنولوجية التي تيسر الاتصال بين الأجهزة والشبكات الإلكترونية، وكذلك بين الأجهزة نفسها. وبفضل ظهور رقائق الكمبيوتر ميسورة التكلفة واتصالات النطاق الترددي العالي أصبحت لدينا الآن مليارات الأجهزة المتصلة بالإنترنت. وهذا معناه أن الأجهزة التي تستخدمها يوميًا يمكنها استخدام أدوات الاستشعار لجمع البيانات والتجاوب بذكاء مع المستخدمين بمعني أن إنترنت الأشياء يدمج الأشياء التي نستخدمها يوميا مثل: مصابيح الإنارة وأجهزة التكييف والمكانس الكهربائية والأبواب والسيارات والآلات مع يمكن إعطاء الأوامر لها لتستجيب وتنفذ هذه الأوامر. وتشكل أجهزة إنترنت الأشياء أجهزة حوسبية، ورقمية، وميكانيكية يمكنها نقل البيانات بشكل مستقل عبر الشبكات الإلكترونية، ومن الأمثلة على هذه الأجهزة أجهزة الكومبيوتر المكتبية والمحمولة، والهواتف المحمولة الذكية، وأجهزة الأمان الذكية وغيرها من الأجهزة، ومع تزايد استخدام أجهزة إنترنت الأشياء من قبل الناس والشركات تزايدت التحديات التي يمكن أن تواجه الأمن السيبراني أيضا، إذ إن الوصول إلى هذه الأجهزة من قبل المخترقين يفسح مجالا واسعا أمام القيام بهجمات مضرة تعرف باسم هجمات إنترنت الأشياء.

المطلب الثالث: آثار تهديدات الأمن السيبراني في البيئة الرقمية.

يمكن أن تؤدي تهديدات الأمن السيبراني إلى تأثيرات ضارة مثل الخسائر المالية وانتهاكات البيانات وسرقة الهوية وانقطاع الخدمات الأساسية، مما يؤثر على الأفراد والشركات والمؤسسات حيث تتطور التهديدات السيبرانية باستمرار، مما يشكل تحديات كبيرة أمام الحفاظ على أمن وسلامة الأنظمة والشبكات الرقمية وتمتد آثار اختراق البيانات لتشمل نطاقًا واسعًا، لا يقتصر على التأثير على الوضع المالي المباشر للشركة فحسب، بل يمتد ليشمل سمعتها وثقة عملائها وسرقة الهوية، وهي نتيجة شائعة للهجمات السيبرانية، قد تسفر عن عواقب وخيمة على الأفراد، ما يؤدي إلى اختراق معلوماتهم الشخصية واضطرابات مالية وقد يتعطل توافر الخدمة بشدة، مما يتسبب في إزعاج واسع النطاق، وقد يُعرّض العمليات الحيوية للخطر وأدى الترابط المتزايد بين المنصات والأجهزة الرقمية إلى خلق منافذ جديدة لمجرمي الإنترنت، مما يجعل من الضروري للأفراد والمؤسسات إعطاء الأولوية لتدابير الأمن السيبراني للحماية من التهديدات المحتملة ومن بين هذه الاثار نجد: (Cyber security threats، 2024)

أ. **خسارة مالية:** يمكن أن تشمل الخسائر المالية الناتجة عن حوادث الأمن السيبراني أضرارًا مالية مباشرة وغرامات تنظيمية ورسومًا قانونية وتكاليف سمعة تؤثر على الشركات والأفراد على حد سواء اذ يمكن أن تُسفر خروقات الأمن السيبراني عن عواقب مالية جسيمة على المؤسسات بمختلف أحجامها. وغالبًا ما تتجاوز التكاليف المرتبطة باختراقات البيانات الأثر المباشر، لتشمل تكاليف التحقيقات الجنائية، وتطبيق التدابير الأمنية، واحتمالية التقاضي ويمكن أن تؤدي مدفوعات الفدية التي يطلبها مجرمو الإنترنت إلى استنزاف الموارد وتعطيل العمليات، كما أن العقوبات التنظيمية المفروضة على انتهاكات حماية البيانات قد تزيد

العبء المالي على الشركات، كما يمكن أن تؤدي هذه الحوادث إلى تراجع ثقة العملاء وولائهم، مما يؤدي إلى عواقب اقتصادية طويلة الأمد.

ب. **خروقات البيانات:** تتضمن خروقات البيانات الوصول غير المصرح به إلى المعلومات الحساسة، مما يؤدي إلى انتهاكات الخصوصية، وكشف البيانات الشخصية، وإساءة الاستخدام المحتملة من قبل الجهات الخبيثة، مما يؤدي إلى تقويض أمن البيانات اذ لا تعرض هذه الخروقات خصوصية الأفراد للخطر فحسب، بل تشكل أيضًا مخاطر جسيمة على المؤسسات. فعندما تقع البيانات الشخصية، كالأسماء والعناوين والمعلومات المالية وأرقام الضمان الاجتماعي، في أيدٍ غير أمينة، قد يقع الأفراد ضحايا لسرقة الهوية والاحتيال ومن منظور مؤسسي، قد تكون عواقب خرق البيانات مدمرة ماليًا، وتضر بالسمعة، وتزعزع الثقة بين العملاء وأصحاب المصلحة. وقد تُفرض أيضًا التزامات قانونية بالإبلاغ عن الاختراقات، وذلك حسب طبيعة الحادثة وحجمها

ج. **سرقة الهوية:** تحدث سرقة الهوية عندما يقوم مجرمو الإنترنت بسرقة المعلومات الشخصية للانخراط في أنشطة احتيالية مثل الاحتيال المالي والاحتيال على الهوية والاستيلاء على الحسابات، مما يشكل مخاطر كبيرة على هويات الأفراد، في العصر الرقمي، ازداد انتشار سرقة الهوية بشكل كبير، حيث تُسهّل خروقات الأمن السيبراني على الجهات الخبيثة اختراق البيانات الحساسة. ويمكن أن تكون عواقب الوقوع ضحية لسرقة الهوية وخيمة، إذ تؤدي إلى خسائر مالية، وتراجع في التصنيف الائتماني، وحتى تشويه السمعة وللتخفيف من هذه المخاطر، ينبغي على الأفراد مراقبة حساباتهم المالية بانتظام، وتفعيل المصادقة الثنائية، وتجنب مشاركة معلوماتهم الشخصية على منصات غير آمنة. ويجب على الشركات الالتزام بلوائح صارمة لحماية البيانات لحماية بيانات العملاء وتجنب مواجهة عواقب قانونية نتيجة الإهمال.

د. **انقطاع الخدمات:** يمكن أن يؤدي انقطاع الخدمات بسبب حوادث الأمن السيبراني إلى تعطل النظام وتوقف العمليات وعدم توفر الخدمة والخسائر المالية، مما يعيق استمرارية الأعمال وثقة العملاء اذ لا تؤثر هذه الانقطاعات على العمليات الداخلية للشركة فحسب، بل تؤثر أيضًا بشكل كبير على قدراتها في خدمة العملاء. عند حدوث انقطاعات في الخدمة، قد يواجه العملاء تأخيرًا في تلقي الدعم أو الوصول إلى المنتجات أو الخدمات التي يعتمدون عليها وقد يؤدي هذا إلى استياء وردود فعل سلبية، بل وحتى فقدان عملاء أوفياء. كما قد تتأثر سمعة المؤسسة سلبًا، إذ ينتشر خبر الحادث الإلكتروني وعواقبه، مما قد يسيء إلى صورة الشركة لدى الجمهور.

المطلب الرابع: التداعيات المستقبلية للأمن السيبراني في البيئة الرقمية وكيفية التغلب على تحدياته.

في عالم أصبحت البيئة الرقمية جزءًا لا يتجزأ من حياتنا اليومية، يزيد الاهتمام بالأمن السيبراني كحاجز دفاعي لحماية المعلومات والأنظمة .ومع تطور التهديدات الإلكترونية وتنوعها، بات من الضروري توقع التداعيات المستقبلية للأمن السيبراني وتطوير استراتيجيات فعّالة للتصدي لها.

الفرع الأول: التداعيات المستقبلية للأمن السيبراني في البيئة الرقمية

من خلال التحليل الموضوعي لمجمل الدراسات العلمية، يتضح أن التداعيات المستقبلية تدور بين مخاوف تفاقم معضلة الدفاع أمام ثغرات الأمن وعدم فعالية الاستراتيجيات المسطرة لغاية الآن لأن التهديدات والهجمات السيبرانية التي تستهدف المرافق المستخدمة للإنترنت في تعاملاتها كالمصارف المالية المؤسسات العمومية، الشركات المتعددة الجنسية ورجال الاعمال، بطريقة وإن كانت متسارعة وخطية، فهذا لا ينفي احتمال توجهها في المراحل المستقبلية المجالات جد حساسة بنفس الطريقة مما يجعل منها جزءا أساسيا في الصراعات العسكرية بين الدول، هذه الاشكاليات تعتبر بالنسبة للمختصين نتاج لمجموعة من الأسباب أو الحقائق، من بينها : افتقار الشركات العاملة في الميدان إلى رؤية صحيحة حول الكيفيات المستعملة في شبكاتها مما سمح للقراصنة بالدخول والخروج بطريقة سهلة، الاستخدام المفرط للوسائط الرقمية، لتوظيف المعلومات، أو إتمام المعاملات، أو غيرها، جعل من هذا المجال الواسع، فجوة لاستهداف المعلومة، خاصة وأن القراصنة يتمتعون بدرجات عالية في المهارات الرقمية، اذ ان مواطن الضعف والعطب في الأمن السيبراني يجسدها الخطأ البشري المتعمد أو غير المتعمد فالمخترعون (البشر) هم من أحدثوا ثورة في التكنولوجيا وأدوات استخدامها وسمحوا للوحدات السياسية (الدول) برعايتها، لكن تبين في الأخير أن الطرفين دخلوا في مواجهة مع الاجرام لن تنتهي بأي حال على المدى القريب. عدم وجود معلومات رسمية كافية ودقيقة حول واقع الأمن السيبراني والتهديدات المتوقعة في البيئة الرقمية، ولم يسمح لأصحاب الاختصاص والمهنيين من تقديم اقتراحات وحلول عملية، وعدم جدية التعاون الاقليمي والدولي فيما يخص تبادل المعلومات والخبرات عدم إدراك ووعي المستخدمين للإعلام وتكنولوجيا الاتصال بمدى تأثير الجرائم الالكترونية على نمط الحياة الشخصية والمهنية حيث اتخذت العديد من الدول إجراءات جديدة لحماية فضاؤها الالكتروني الخاص بالقوات المسلحة على غرار الصين التي استبقت الاحداث وأنشأت الجيش الازرق)،التي يمكن إلى حد ما اعتبارها مؤشرات دالة على أن العالم في ثوبه الجديد (عالم بالا أقطاب) يستعد لمواجهة إفرازات حرب إلكترونية متوقعة بين الحين والآخر. (بوازدية، 2021، الصفحات 23-24)

الفرع الثاني: كيفية التغلب على تحديات وتهديدات الأمن السيبراني.

لتغلب على تحديات وتهديدات الأمن السيبراني، يجب التأكيد من نهج الأمن السيبراني الناجح يجب أن يحتوي على طبقات متعددة من الحماية تنتشر عبر أجهزة الحاسب الآلي أو الشبكات أو البرامج أو البيانات التي يرغب المرء في الحفاظ عليها وحمايتها من أي تلاعب أو ضرر وبالنسبة للأشخاص والعمليات والتكنولوجيا فإنه يجب أن يكمل كل منها الآخر داخل الشركة أو المؤسسة لإنشاء نظام دفاع متكامل وفعال في مواجهة الهجمات والجرائم السيبرانية. ويمكن لنظام إدارة التهديدات السيبرانية الموحد تسريع وظائف عمليات الأمان الرئيسية التالية: اكتشاف والمواجهة والدفاع والمعالجة والتحقق وهناك أمور عديدة إذا تم مراعاتها وتطبيقها يمكن في هذه الحالة الوقاية من تحديات الأمن السيبراني أو مواجهة هذه التحديات في حال حدوثها، من هذه الأمور: (الخبيزي، 2023، الصفحات 246-248)

أولا: **الأشخاص**:

أ. ضرورة عقد دورات تدريبية للمستخدمين في مجال الأمن السيبراني، على أن تتناول مفاهيم وأهداف وأهمية وفوائد وأنواع الأمن السيبراني والتحديات التي تواجهه وكيفية التغلب عليها.

ب. ضرورة عقد ورش عمل حول إجراءات الحماية ضد تحديات وتهديدات ومخاطر الأمن السيبراني تحت اشراف مدربين مختصين في الأمن السيبراني

ج. يجب على المستخدمين فهم المبادئ الأساسية الأمان البيانات والمعلومات والامتثال إليها مثل اختيار كلمات مرور قوية والحذر من المرفقات الموجودة ضمن البريد الإلكتروني والنسخ الاحتياطي للبيانات.

ثانيا: **العمليات**:

أ. يجب أن تمتلك المؤسسات إطار عمل حول كيفية التعامل مع الهجمات السيبرانية غير المكتملة أو الناجحة .

ب. وضع إطار عمل موحد يوضح كيف يمكنك تحديد الهجمات السيبرانية وحماية الأنظمة واكتشاف التهديدات والتصدي لها والتعافي من الهجمات الناجحة.

ثالثا: **التقنية**

أ. توفير التكنولوجيا هو أمر ضروري لمنح المؤسسات والأفراد أدوات الأمن السيبراني اللازمة لحماية أنفسهم من الجرائم والهجمات السيبرانية .

ب. يجب أن توجه الحماية للكيانات التالية: الأجهزة الطرفية مثل أجهزة الكمبيوتر والأجهزة الذكية والموجهات والشبكات والسحابة

ج. ومن أشكال التكنولوجيا الشائعة المستخدمة لحماية هذه الكيانات الجيل التالي من الجدران النارية وتصفية DNS و الحماية ضد البرامج الضارة وبرامج مكافحة الفيروسات وحلول أمان البريد الإلكتروني .

رابعا: **المجتمع** :

أ. ضرورة توعية المجتمع بأهمية الأمن السيبراني وبأساليب الحماية من التهديدات والمخاطر التي تواجه الأمن السيبراني، وذلك من خلال وسائل الاتصال الجماهيرية وخاصة التليفزيون والصحف.

ب. ضرورة تشجيع المواطنين عن الإبلاغ عن الجرائم السيبرانية .

ج. ضرورة وضع وتطوير تشريعات حديثة لمكافحة الهجمات والجرائم السيبرانية .

د. إعداد مصفوفة للمعايير الأخلاقية فيما يتعلق باستخدام النظم الإلكترونية .

هـ. تخصيص اختصاص قضائي خاص بهذه النوعية من الهجمات والجرائم السيبرانية.

و. ضرورة التنسيق بين الأجهزة الأمنية لمكافحة الهجمات والجرائم السيبرانية.

ز. إنشاء مراكز وطنية مسئولة عن حماية الأمن السيبراني للدولة وتدعيمها بالخبراء من مختلف التخصصات المرتبطة مثل: المركز الوطني للأمن السيبراني بالكويت والمركز الوطني الارشادي للأمن السيبراني بالمملكة العربية والسعودية والهيئة الوطنية للأمن الإلكتروني بالإمارات.

خلاصة الفصل:

في ختام هذا الفصل الذي تناول عموميات حول الأمن السيبراني والبيئة الرقمية، يتضح أن التحول الرقمي السريع قد أحدث ثورة في مختلف مجالات الحياة، مما جعل البيئة الرقمية جزءًا لا يتجزأ من الواقع المعاصر .وقد أتاح هذا التحول فرصًا هائلة للتطور والابتكار، إلا أنه جلب معه تحديات أمنية متزايدة تتطلب اهتمامًا خاصًا حيث ان الأمن السيبراني يقوم بحماية الأنظمة الرقمية والشبكات والبيانات من التهديدات الإلكترونية المتنوعة، مثل الهجمات السيبرانية والاختراقات والبرمجيات الخبيثة ويتطلب ذلك تبني استراتيجيات وتقنيات متقدمة لضمان سرية المعلومات وسلامتها وتوافرها .

تتعدد التحديات التي تواجه الأمن السيبراني، منها التهديدات المتطورة، ونقص الكفاءات المتخصصة، والحاجة إلى تحديث الأنظمة باستمرار ولمواجهة هذه التحديات، يجب تعزيز الوعي الأمني، وتطوير السياسات والتشريعات المناسبة، والاستثمار في التدريب والتقنيات الحديثة حيث إن الحفاظ على أمن البيئة الرقمية هو مسؤولية مشتركة تتطلب تعاونًا بين الأفراد والمؤسسات والحكومات، لضمان بيئة رقمية آمنة ومستدامة تدعم الابتكار والتقدم في مختلف المجالات.

الفصـــــــــل الثـــــاني

واقع الأمن السيبراني ودوره في تحسين البيئة الرقمية في جامعة محمد خيضر بسكرة

تمهيد:

بعد التطرق في الفصل السابق إلى الإطار النظري الذي يحيط بإشكالية البحث، يأتي هذا الفصل لاستكمال العمل العلمي من خلال الجانب التطبيقي، وذلك عبر دراسة ميدانية أُجريت بجامعة محمد خيضر – بسكرة، حيث تم توزيع استبيان الدراسة على عيّنة من أساتذة الجامعة، وقد تم اختيار هذه المؤسسة نظرًا لخصوصية نشاطها الأكاديمي، وتميزها في توظيف الرقمنة في مختلف جوانب العمل الجامعي.

ويهدف هذا الفصل إلى الربط بين ما طُرح في الإطار النظري، وما يمكن تحليله وتفسيره ميدانيًا داخل بيئة الجامعة، من أجل الوصول إلى نتائج تعكس الواقع الفعلي للعلاقة بين الأمن السيبراني والبيئة الرقمية وقد تم تقسيم هذا الفصل إلى ثلاث مباحث كمايلي:

- **المبحث الأول : نظرة عامة حول جامعة محمد خيضر بسكرة.**
- **المبحث الثاني: الطريقة والأدوات المتبعة في الدراسة.**
- **المبحث الثالث : نتـائج دراسـة تحليل الاستبيان.**

المبحث الأول: نظرة عامة حول جامعة محمد خيضر بسكرة.

يُعدّ التعرف على الإطار المؤسساتي للدراسة أمرًا ضروريًا لفهم سياقها العام، لذلك سنتناول في هذا المبحث نظرة شاملة حول جامعة محمد خيضر – بسكرة، من حيث النشأة، والمصالح التابعة لها.

المطلب الأول: نشأة جامعة محمد خيضر بسكرة.

جامعة محمد خيضر بسكرة هي مؤسسة عمومية ذات طابع علمي و ثقافي و مهني تتمتع بالشخصية المعنوية و الاستقلالية ، و تتشكل جامعة محمد خيضر بسكرة من هيأت (مجلس الادارة و مجلس علمي) ، رئاسة الجامعة ،كليات و معاهد و ملحقات في بعض الاحيان ،كما تتضمن مصالح ادارية و تقنية مشتركة ، و فيما يلي مراحل نشأة جامعة محمد خيضر بسكرة :

أ. **المرحلة الاولى : مرحلة المعاهد (1984–1992)** :كانت المعاهد الوطنية تتمتع باستقلالية ادارية ، بيداغوجية و مالية و تتكفل هيئة مركزية بالتنسيق بينها

- المعهد الوطني للري (المرسوم رقم 254- المؤرخ في : 1984/18/08).
- المعهد الوطني للهندسة المعمارية (المرسوم رقم 253-84 المؤرخ في : 1984/08/05) .
- بالإضافة الى المعهد الوطني للكهرباء التقنية في عام 1986 (المرسوم رقم : 169-86 المؤرخ في : 1/08/18ك 986) .

ب. **المرحلة الثانية : مرحلة المركز الجامعي (1992–1998)** :تحولت هذه المعاهد الى مركز جامعي بمقتضى المرسوم رقم : 295-92 المؤرخ في : 1992/07/07 .

منذ عام 1992 تم فتح معاهد اخرى :

- معهد العلوم الدقيقة
- معهد الهندسة المدنية
- معهد العلوم الاقتصادية
- معهد الالكترونيك
- معهد الادب العربي
- معهد علم الاجتماع

ج. **المرحلة الثالثة : مرحلة الجامعة (1998 الى يومنا هذا)** : بصدور المرسوم رقم 219-98 المؤرخ في : 1998/07/07 تحول المركز الجامعي الى جامعة تضم 03 كليات .

ثم في 24 /2004/08 صدر المرسوم التنفيذي رقم : 255-04 المعدل للمرسوم التنفيذي رقم 219-98 المؤرخ في : 1998/07/07و المتضمن انشاء جامعة بسكرة ، المعدل بحيث اصبحت الجامعة تتكون من اربع (04) كليات هي :

- كلية العلوم و علوم المهندس
- كلية الآداب و العلوم الانسانية و العلوم الاجتماعية
- كلية الحقوق و العلوم السياسية
- كلية العلوم الاقتصادية و التسيير

د. **الوضعية الحالية** : ثم جاء المرسوم التنفيذي رقم : 90-09 المؤرخ في : 21 صفر 1430 الموافق ل : 17 فبراير 2009، الذي يعدل و يتمم المرسوم التنفيذي رقم 219-98 المؤرخ في : 1998/07/07 و اصبحت الجامعة تتكون من ست (06) كليات :

- كلية العلوم الحقيقة و علوم الطبيعة و الحياة : قسم الرياضيات ، قسم الاعلام الالي ، قسم علوم المادة ، قسم علوم الارض و الكون ، قسم العلوم البيولوجية ، قسم العلوم الزراعية .
- كلية العلوم و التكنولوجيا : قسم هندسة الطرائق ، قسم الهندسة المدنية و الري ، قسم الهندسة الكهربائية ، قسم الهندسة المعمارية .
- كلية الحقوق و العلوم السياسية .
- كلية العلوم الانسانية و الاجتماعية .
- كلية العلوم الاقتصادية و التجارية و علوم التسيير .
- كلية الآداب و اللغات .

كما عدل المرسوم التنفيذي المادة 4 من المرسوم التنفيذي رقم 98-219 بحيث اصبحت تضم مديرية الجامعة زيادة على الامانة العامة و المكتبة المركزية اربع (04) نيابات مديرية تكلف على التوالي بالميادين الاتية :

- نيابة مديرية الجامعة للتكوين العالي في التدرج و التكوين المتواصل و الشهادات
- نيابة مديرية الجامعة للتكوين العالي فيما بعد التدرج و التأهيل الجامعي و البحث العلمي .
- نيابة مديرية الجامعة للعلاقات الخارجية و التعاون و التنشيط و الاتصال و التظاهرات العلمية .
- نيابة مديرية الجامعة للتنمية و الاستشراف و التوجيه .

المطلب الثاني: هيكلة النظام البيداغوجي للجامعة.

تتكون جامعة محمد خيضر بسكرة من اربع نيابات و ست كليات و معهد جامعي بالمرسوم التنفيذي رقم 14-129 الموافق 05 افريل 2014 يعدل و يتمم المرسوم التنفيذي رقم 98-219 الموافق ل 07 جويلية 1998 و المتضمن انشاء جامعة بسكرة و هو كالاتي :

أ. **نيابات رئاسة الجامعة:**

- التكوين العالي في الطورين الاول و الثاني و التكوين المتواصل و الشهادات و كذا التكوين العالي في التدرج
- التكوين العالي في الطور الثالث و التاهيل الجماعي و البحث العلمي و كذا التكوين العالي فيما بعد التدرج
- العلاقات الخارجية و التعاون و التنشيط و الاتصال و التظاهرات العلمية
- التنمية و الاستشراف و التوجيه

ب. **الكليات** : تتكون جامعة محمد خيضر بسكرة من ست (06) كليات و معهد و 32 قسم

- كلية العلوم الحقيقة و علوم الطبيعة و الحياة : قسم الرياضيات ، قسم الاعلام الالي ، قسم علوم المادة ، قسم علوم الارض و الكون ، قسم العلوم البيولوجية ، قسم العلوم الزراعية .

- كلية العلوم و التكنولوجيا : قسم هندسة الطرائق ، قسم الهندسة المدنية و الري ، قسم الهندسة الكهربائية ، قسم الهندسة المعمارية .
- كلية الحقوق و العلوم السياسية : قسم الحقوق ، قسم العلوم السياسية
- كلية العلوم الانسانية و الاجتماعية : قسم العلوم الانسانية ، قسم العلوم الاجتماعية .
- كلية العلوم الاقتصادية و التجارية و علوم التسيير : قسم العلوم الاقتصادية ، قسم العلوم التجارية ، قسم علوم التسيير
- كلية الاداب و اللغات : قسم اللغة و الادب العربي ، قسم الاداب و اللغات الاجنبية .

ج. **المعهد** :

معهد علوم و تقنيات النشاطات البدنية و الرياضية :

- قسم الادارة و التسيير الرياضي .
- قسم التدريب الرياضي .
- قسم التربية الحركية .

د. **المصالح المشتركة** :

- مركز الانظمة و شبكات الاعلام الالي و الاتصال و التعليم المتلفز و التعليم عن بعد
- مركز تعليم تكثيف اللغات
- المركز السمعي البصري
- البهو التكنولوجي
- خلية ضمان الجودة
- دار المقاولتية

هـ. **الهياكل البيداغوجية** :

- تتربع جامعة محمد خيضر بسكرة على مساحة تقدر ب 126.2392 هكتارا و تتكون من الربعة (4) مجمعات .
- و تتوفر جامعة بسكرة على 23816 مقعد بيداغوجي.
- بالنسبة للمدرجات 29 بطاقة استعياب 5610 .
- و قاعات التدريس و الاعمال التوجيهية 386 بطاقة استعياب 11341.
- الاعمال التطبيقية 50 بطاقة استعياب 620 .
- قاعات الرسم و الورشات 18 بطاقة استعياب 660 .
- قاعات المحاضرات الكبرى 02.
- قاعات الحساب 08 قاعات الانترنت 170 .
- قاعات المحاضرات المرئية (visioconférences) : 01 .
- قاعات التعليم عن بعد (télé-enseignement) :01.

المطلب الثالث : البيئة الرقمية في جامعة محمد خيضر بسكرة.

تستخدم جامعة محمد خيضر بسكرة تكنولوجيا المعلومات و الاتصال من خلال :

أ. **مركز الانظمة و شبكات الاعلام الالي و الاتصال و التعليم المتلفز و التعليم عن بعد** :تعتبر شبكة الانترنت للجامعة جزء من الشبكة الوطنية ARN الشبكة الاكادمية للبحث ، و هي مرتبطة بالشبكة الاروبية GEANT و هي حاليا بتدفق 100 ميغابايت ، شبكة الانترنت للجامعة عبارة عن ربط لثلاثة مواقع بواسطة الالياف البصرية و تكنولوجية اللاسلكي ، و قد ارتفع عدد الوصلات لاكثر من 820 وصلة و ما يقارب 30 جهاز لاسلكي ، تغطي جميع مرافق و هياكل الجامعة ، باستثناء القطب الحاجب و مركز البحث العلمي اين تم برمجة ربط هذه المواقع ب 3400 وصلة خلال هذه السنة ، فتح قاعات جديدة للانترنت للاعلام الالي و تجهيزيها ، حيث اصبح حوالي 350 جهاز الاعلام الي يستفيد منه الطلبة في جميع الاوقات مع توفير خدمة الويفي wifi و wi-ssi

ب. **خدمات الانترنت و الانترانت** : يحرص مركز الشبكات للجامعة على حسن تسيير هذه الشبكة و تثبيت و صيانة الخوادم (Serveurs) ، و كذلك يقدم المركز الخدمات التالية : منح البريد الالكتروني (Email) للمشتركين ، حوالي 1000 مشترك ، استفادة الاساتذة الباحثين الجزائرين من خدمة النظام الوطني للتوثيق الالكتروني SNDL بالجامعات الجزائرية ، التعلم عن بعد حيث يحتوي على مواد بيداغوجية و هو اداة مكملة للتعليم الحضوري و تحتوي المنصة (Plate forme)على حوالي 123 درس ، التعليم المتلفز visio-conférence تم انجاز و ارسال 02 محاضرة مرئية ، ادراج وتسسير التظاهرات العلمية من اجل تسهيل عملية المشاركة في التظاهرات العلمية ، المكتبة الرقمية حيث تحتوي على الاطروحات و المذكرات التي نوقشت بالجامعة ، و يتم البحث عن الكتب و المراجع بطريقة رقمية ذكية ،كما تمت الاستفادة من الشبكة في عملية تسجيل حاملي شهادة الباكالوريا .

المطلب الرابع: اعضاء هيئة التدريس في جامعة محمد خيضر بسكرة .

حسب موقع الجامعة فان عدد اعضاء هيئة التدريس في جامعة محمد خيضر بسكرة قد بلغ 1497 أستاذ و أستاذة مصنفين حسب تخصصهم حيث بلغ عدد الاساتذة في كلية العلوم الاقتصادية و التجارية و علوم التسيير 196 أستاذ و أستاذة ، و بلغ عدد أساتذة كلية العلوم الانسانية و الاجتماعية 165 أستاذ و أستاذة ، و بلغ عدد اساتذة كلية الحقوق و العلوم السياسية 125 أستاذ و أستاذة ، و بلغ عدد أساتذة كلية الآداب و اللغات 202 أستاذ و أستاذة ، و بلغ عدد أساتذة كلية كلية العلوم الحقيقة و علوم الطبيعة و الحياة 365 أستاذ و أستاذة ، و بلغ عدد اساتذة كلية العلوم و التكنولوجيا 414 أستاذ و أستاذة ، و بلغ عدد أساتذة معهد علوم و تقنيات النشاطات البدنية و الرياضية 30 أستاذ .

الجدول رقم (01) : جدول يوضح توزيع أساتذة جامعة محمد خيضر بسكرة حسب الكلية

الكلية	عدد الأساتذة
كلية العلوم الاقتصادية و التجارية و علوم التسيير	**32** أستاذ و**54** استاذة
كلية العلوم الانسانية و الاجتماعية	**78** أستاذ و **87** أستاذة
كلية الحقوق و العلوم السياسية	**63** أستاذ و **62** أستاذة
كلية الاداب و اللغات	**104** أستاذ و**98** أستاذة
كلية العلوم الحقيقية و علوم الطبيعة و الحياة	**225** أستاذ و**140** أستاذة
معهد علوم و تقنيات النشاطات البدنية و الرياضية	**30** أستاذ

المصدر: من اعداد الطالبة اعتمادا على معلومات المجمعة.

المبحث الثاني: الطريقة والأدوات المتبعة في الدراسة.

سنتطرق في هذا المبحث إلى عرض مجتمع وعينة الدراسة وخطوات بناء الاستبيان والتحقق من الأدوات المستخدمة بالإضافة إلى الأدوات الإحصائية المستخدمة فيها.

المطلب الأول: اداة الدراسة وأساليب احصائية.

في هذا المطلب نسلط الضوء على إجراءات الدراسة وذلك من خلال إعطاء لمحة موجزة عن مجتمع وعينة الدراسة، ومن ثم سنتعرف على مصادر جمع المعلومات لهذه الدراسة ويعتبر تحديد مجتمع الدراسة أهم خطوة في الدراسة التطبيقية لارتباطه المباشر بهدفها ونتائجها، وللحصول على دراسة تتسم بالدقة وذات مصداقية لابد وأن يكون أفراد المجتمع المختار من ذوي الخبرة في الميدان العملي، وبذلك يتمثل مجتمع البحث في جميع أساتذة جامعة محمد خيضر بسكرة.

فيما يتعلق بعينة الدراسة البالغ عددها حوالي 50، حيث اعتمدنا طريقة العينة العشوائية البسيطة في اختيار عينة البحث، وقد تم توزيع الإستبانة عليهم من خلال عدة زيارات للكليات، واسترجعنا منها 39 استبانة، وبعد جمع وفحص الاستبانات المسترجعة وتدقيقها حتى تستوفي الشروط اللازمة للمعالجة الإحصائية، أصبحت 36 استبانة صالحة للتحليل الإحصائي، وهو عدد جيد مقبول لأغراض البحث العلمي، وكان سبب عدم تمكن الطالب من إسترجاع النسبة المتبقية هو عدم تمكن بقية الموظفين من الإجابة على الاستبيان بسبب الضغوطات وانشغالاتهم. والجدول أدناه يوضح عدد الإستبانات الموزعة و المسترجعة من عينة الدراسة.

الجدول رقم(02): الاستبيانات الموزعة والمسترجعة من عينة الدراسة

الاستبانات	عدد الاستبانات	النسبة المئوية
الاستبانات الموزعة	50	100%
الاستبانات المسترجعة	40	%80
الاستبانات غير قابلة للتحليل	04	%8
الاستبانات الصالحة للتحليل	36	%72

المصدر: من إعداد الطالبة بناء على النتائج المتحصل عليها من جمع الاستبانات.

ولجمع المعلومات حول موضوع الدراسة تم استخدام مصدرين رئيسين هما:

1. **المصادر الأولية** : لمعالجة الجوانب التحليلية المتعلقة ب: **"دور الأمن السيبراني في تحسين البيئة الرقمية دراسة حالة حول تحديات الحماية الرقمية في جامعة بسكرة "**، تم القيام بإعداد الإستبيان الملحق بهذه الدراسة كأداة رئيسية لجمع المعلومات اللازمة حيث صمم خصيصا لهذا الغرض ووزع على 50 أستاذ من الجامعة.
2. **المصادر الثانوية**: قامت الطالبة لمعالجة الإطار النظري للدارسة على مجموعة من مصادر البيانات الثانوية التي تخدم موضوع الدراسة سواء بطريقة مباشرة أو غير مباشرة و تتمثل هذه المصادر في الكتب، المذكرات، المقالات، المجلات، ذات صلة بالموضوع.

3. **أداة الدراسة**: تماشيا مع طبيعة الموضوع الذي نحن بصدد دراسته، وبغرض جمع البيانات اللازمة للإجابة عن تساؤلات الدراسة واختبار فرضياتها، اعتمدنا في هذه الدراسة على الاستبيان كأداة دراسة أساسية لجمع المعلومات والبيانات الخاصة بعينة الدراسة.

وبعد الاطلاع على الدراسات السابقة وتحديد أبعاد الموضوع، تم تصميم الاستبيان وفقا لما أملته علينا المعطيات سابقة الذكر، بحيث اشتمل على مجموعة من العبارات المندرجة تحت محاور وأبعاد الدراسة التالية:

أ- **القسم الأول**: يتعلق بالمعلومات الشخصية لأفراد العينة ويتكون من خمس عبارات المتمثلة في (الجنس، العمر، الكلية، سنوات الخبرة، الرتبة الوظيفية).

ب- **القسم الثاني**: والذي يتعلق بموضوع الدراسة **دور الأمن السيبراني في تحسين البيئة الرقمية دراسة حالة جامعة محمد خيضر بسكرة**، حيث ينقسم هذا الأخير إلى محورين هما:

- **المحور الأول**: المتعلق بالمتغير المستقل **الأمن السيبراني** ، حيث يضم 12 عبارة.
- **المحور الثاني**: والمتعلق بالمتغير التابع **البيئة الرقمية**، حيث يضم 16 عبارة ، قسمت الى ثلاثة أبعاد كالتالي: **البنى التحتية الرقمية، المهارات الرقمية، الثقافة الرقمية**.

استخدمت الطلبة مقياس ليكرت الخماسي لتحديد أوزان فقرات الاستبيان والذي يتضمن 05 علامات (غير موافق بشدة، غير موافق، محايد، موافق، موافق بشدة) كما هو موضح بالجدول أدناه

الجدول رقم(03): درجات مقياس ليكرت

درجات الإستجابة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
رقم الدرجة	1	2	3	4	5

المصدر: من إعداد الطالبة اعتمادا على دراسات سابقة

تم تحديد الحدود العليا و الدنيا لمقياس ليكرت الخماسي وهذا من خلال تحديد طول فئات المقياس المستخدم في محاور الدراسة عن طريق حساب المدى (**5-1=4**)، ومن ثم تقسيمه إلى عدد فئات المقياس للحصول على طول الفئة الصحيح أي (**4/5=0.8**)بعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس والمتمثلة في الواحد الصحيح وذلك لتحديد الحد الأعلى لهذه الفئة وهكذا أصبح طول الفئات كما يوضحه الجدول التالي:

الجدول رقم(04): جدول يوضح طول الخلية لسلم ليكرت

الفئـــات	درجـــة الموافقـــة
(1 -1.79)	**غير موافق بشدة**
(1.80 -2.59)	**غير موافق**
(2.60 -3.39)	**محـايد**
(3.40 -4.19)	**موافق**
(4.20 -5)	**موافق بـشدة**

المصدر: من إعداد الطلبة بالاعتماد على دراسات سابقة

4. **الأساليب الإحصائية المستخدمة في الدراسة.**

في إطار إجراء معالجة وتحليل للبيانات المتحصل عليها، سيتم الاعتماد على برنامج الحزم الإحصائية للعلوم الاجتماعية (**SPSS**) إصدار26 الذي تم من خلاله دراسة وتحليل العلاقة بين المتغير المستقل **الامن السيبراني** والمتغير التابع **البيئة الرقمية**، بحيث تتمثل أهم الاختبارات المعتمدة في الدراسة كالآتي:

أ. **معامل ألفا كرونباخ (Alpha Cronbach Test)**: للتأكدمن مدى ثبات فقرات الاستبيان.

ب. **التكرارات والنسب المئوية**: لغرض التعرف على تكرار فئات متغير ما، ويفيد في وصف عينة الدراسة.

ج. **المتوسطات الحسابية**: لمعرفة اتجاهات إجابات أفراد عينة الدراسة، ومتوسط محتوى المحاور والأبعاد والعبارات.

د. **الانحرافات المعيارية**: للتعرف على مدى انحراف استجابات أفراد عينة الدراسة المتعلقة بالعبارات والمحاور الأساسية لمتغيراتها.

هـ. **معـامل الإلتواء ومعامل التفلطح**: لمعرفة مدى إتباع البيانات لتوزيع الطبيعي.

و. **معامل الارتباط بيرسون (Pearson)**: يستعمل لقياس صدق أداة الدراسة، وأيضاً دراسة مختلف علاقات الارتباط بين محاور متغيرات الدراسة.

ز. **اختبار الانحدار البسيط (Simple Regression Test)**: لدراسة أثر كل محور من محاور المتغير المستقل على المتغير التابع.

المطلب الثاني: صدق و ثبات الاستبيـان.

لتحكيم في صدق أداة الدراسة تم استخدام طريقتين وهما: الصدق الظاهري (المحكمين) الصدق الذاتي (صدق الاتساق الداخلي)

أولا: **الصدق الظاهري لأداة الدراسة.**

يقصد بصدق اختبار الأداة مدى تناسق فقرات الاستبيان مع متغيرات الدراسة التي تعمل على قياسها وأن مضمونها يتفق مع الغرض الذي صممت من أجله، لذا وللتحقق من صدق محتوى أداة البحث ومدى تغطيتها لأبعاد الرئيسية لموضوع الدراسة، تم مراجعتها وتصحيحها من قبل الأستاذ المشرف، وفي ضوء ملاحظاته وتوجيهاته تم إجراء التعديلات المطلوبة من حيث إعادة الصياغة أو حذف بعض العبارات وإضافة عبارات جديدة بشكل يحقق التوازن بين مضامين الأداة في فقراتها لنتحصل على الاستبيان في صورته النهائية (الملحق رقم01.).

ثانيـا: **الصدق الذاتـي لأداة الدراسة**

الصدق الذاتي لأداة الدراسة يهدف إلى تحديد مدى تجانس الاستبيان وتناسقه الداخلي، وللقيام بهذا الاختبار قمنا بحساب معامل الارتباط بيرسون (**Pearson**)، بين كل عبارة من عبارات الاستبيان والبعد الذي تنتمي إليه وقد تحصلنا على النتائج المبينة في الجدوال الآتية:

1. الصدق الداخلي للمحور الاول: الأمن السيبراني.

يهدف هذا العنصر إلى التحقق من صدق الاتساق الداخلي لعبارات المحور الأول المتعلق بالأمن السيبراني، والذي يتضمن 12 عبارة وبالاستناد إلى نتائج الجدول الموالي، يتضح أن غالبية قيم معاملات الارتباط المحسوبة كانت موجبة ودالة إحصائيًا عند مستوى 0.05 أو أقل، مما يشير إلى وجود علاقة ارتباط معنوية بين العبارات والمحور الذي تنتمي إليه. وقد تراوحت معاملات الارتباط بين (*0.417 - **0.772)، وهي تشير إلى ارتباط بدرجة متوسطة إلى قوية، كما ان اغلب القيم متميزة بنجوم التي تدل أن النتيجة ذات دلالة إحصائية عالية عند مستوى 0.001 وهذا يعني أن هناك أقل من 1% احتمال أن تكون النتيجة بسبب الصدفة، مما يشير إلى دلالة إحصائية قوية وبالتالي فان العبارات الموضوعة في هذا المحور صادقة لما وصفت لقياسه مما يعزز من صدق العبارات الموضوعة لقياس هذا المحور

الجدول رقم(05) : يوضح الصدق الداخلي لعبارات المحور الاول باستخدام معامل الارتباط لبيرسون.

رقم العبارات	العبارات	معامل الإرتباط	مستوى الدلالة
.1	توجد سياسة واضحة للأمن السيبراني في المؤسسة الجامعية.	.417*	.011
.2	تنظيم تدريبات للموظفين على أساسيات الأمن السيبراني بشكل منتظم.	.606**	.000
.3	استخدام برامج وتطبيقات موثوقة للحماية من الاختراقات والبرمجيات الخبيثة	.750**	.000
.4	يُسمح فقط باستخدام البرمجيات المعتمدة على الأجهزة الجامعية.	.540**	.001
.5	ايجاد اليات للإبلاغ عن التهديدات الأمنية الرقمية اتصال خارجية.	.745**	.000
.6	يتم اتخاذ إجراءات فعلية بعد الإبلاغ عن التهديدات أو الحوادث الأمنية	.677**	.000
.7	تعتقد أن الطلاب والموظفين بحاجة إلى برامج توعوية مستمرة حول الأمن السيبراني	.725**	.000
.8	يتم تحديث الأنظمة التشغيلية والتطبيقات بانتظام داخل الجامعة	.651**	.000
.9	تعتقد أن الشبكة الداخلية للجامعة آمنة بما فيه الكفاية	.772**	.000
.10	تترك أجهزتك مفتوحة أو غير مؤمّنة عند الابتعاد عنها	.584**	.000
.11	تقوم بفحص الروابط أو المرفقات قبل فتحها عبر البريد الإلكتروني	.633**	.000
.12	تستخدم كلمات مرور قوية ومختلفة لحساباتك الجامعية.	.111	.519

المصدر: من إعداد الطالبة بالاعتماد على مخرجات SPSS V 26

2. **الصدق الداخلي لأبعاد المحور الثاني: البيئة الرقمية.**

من خلال هذا العنصر يتم توضيح صدق الاتساق لكل بعد من أبعاد **البيئة الرقمية** مع المحور نفسه كمايلي و الذي يضم 16 عبارة من خلال الجدول الموالي بحيث نرى أن جميع قيم معاملات الارتباط المبنية موجبة و دالة عند مستوى 0.05 او أقل، وعليه بالاعتماد على نتائج المسجلة تعتبر أبعاد محور الاول (**البنية التحتية الرقمية/ المهارات الرقمية/ الثقافة الرقمية**) مرتبطة ارتباطا قويا مع محور **البيئة الرقمية** وذلك لأنها محصورة بين معامل ارتباط (0.479**- 0.906**) ومتميزة بنجوم التي تدل أن

النتيجة ذات دلالة إحصائية عالية عند مستوى 0.001 وهذا يعني أن هناك أقل من 1% احتمال أن تكون النتيجة بسبب الصدفة، مما يشير إلى دلالة إحصائية قوية وبالتالي فان العبارات الموضوعة في هذا المحور صادقة لما وصفت لقياسه.

الجدول رقم (06) : يوضح الصدق الداخلي لأبعاد المحور الثاني باستخدام معامل الارتباط لبيرسون.

البعد	عنوان البعد	معامل الإرتباط	مستوى الدلالة
البعد الاول	**– البنية التحتية الرقمية**	.906**	**0.000**
البعد الثاني	**– المهارات الرقمية**	.900**	**0.000**
البعد الثالث	**– الثقافة الرقمية**	.479**	**0.003**

المصدر: من إعداد الطلبة بالاعتماد على مخرجات spss 26

ثالثا:ثبات الاستبيان

من أجل قياس مدى ثبات أداة الدراسة (الاستبيان) تم الاستعانة بالبرنامج الإحصائي"**SPSS** " من خلال استعمال معامل "**ألفا كرونباخ** "للتحقق من صحة وثبات عبارات الاستبيان، وكانت نتائج كما هي مبينة في الجدول:

الجدول رقم(07): معامل ألفا كرونباخ لقياس ثبات محاور الاستبيان

المحاور الدراسية	الأبعاد	عدد الفقرات	معامل ألفا كرونباخ
المحور الأول	**الأمن السيبراني**	**12**	**0.847**
المحور الثاني	**– البنى التحتية الرقمية**	**06**	**0.803**
	– المهارات الرقمية.	**05**	**0.702**
	– الثقافة الرقمية	**05**	**0.266**
	البيئة الرقمية	**16**	**0.688**
عبارات الاستبيان ككل		**28**	**0.906**

المصدر: من إعداد الطلبة بالاعتماد على مخرجات spss26

- يتضح من خلال الجدول أعلاه أن معامل الثبات (ألفا كرونباخ) لجميع "**عبارات الأمن السيبراني**" ككل (0.847) وهي قيمة مرتفعة وجيدة ملائمة للدراسة حيث أظهرت أعلى مستوى من الثبات، مما يعزز من موثوقية الأداة في قياس محور الامن السيبراني.
- بينما معامل الثبات (ألفا كرونباخ) لأبعاد المحور الثاني قد تراوحت ما بين (0.803/0.266) وهي قيم مقبولة، في حين بلغت قيمة معامل ثبات (ألفا كرونباخ) لجميع "**عبارات البيئة الرقمية**" ككل (0.688) وهي تعد قيمة مقبولة وملائمة للدراسة وبهذا أظهرت معظم نتائج المحور الثاني مستويات جيدة من الثبات، الا البعد الثالث الذي كات قيمة الفا كرونباخ لديه (0.266) لكن ما يهم هو قيمة البعد ككل والتي كانت مقبولة وهذا يعني أنها العبارات موثوقة لقياس هذه الجوانب.

- أما فيما يخص معامل الثبات الإجمالي لعبارات الاستبيان ككل فقد بلغت قيمته (0.906) وهي قيمة مرتفعة و جيدة مما يعكس جودة وفعالية الأداة المستخدمة في قياس المحاور المختلفة للاستبيان.

وبما أن معامل الثبات ألفا كرونباخ في إجمالي محاور الاستبيان، كانت أكبر من الحد الأدنى أي من 0.60، يمكن القول أن أداة الدراسة **صادقة وثابتة** في جميع عباراتها، وهي جاهزة للتطبيق على عينة الدراسة.

المطلب الثالث: اختبار التوزيع الطبيعي .

سنقوم باختبار التوزيع الطبيعي لمتغيرات الدراسة، وهو عنصر ضروري لاختبار الفرضيات، للتأكد من خضوع بيانات الدراسة للتوزيع الطبيعي أم لا. حيث يتم احتساب قيمة معامل الالتواء ومعامل التفلطح للمتغيرات، ويجب أن تكون هذه القيم محصورة ما بين [-3، 3] بالنسبة لمعامل الالتواء، وما بين [-7، 7] بالنسبة لمعامل التفلطح والجدول أدناه يوضح حساب قيم الالتواء والتفلطح للإجابات المتعلقة بالأبعاد المكونة لكل متغير من متغيرات الدراسة.

الجدول رقم(08): جدول يوضح نتائج معامل الإلتواء ومعامل التفلطح لمتغيرات الدراسة

متغيـــــرات الدراســـة	معامل الالتواء (Skewness)		معامل التفلطح (Kurtosis)	
	الاحصائيات	الخطأ المعياري	الاحصائيات	الخطأ المعياري
الأمن السيبراني	-.919	.393	1.643	.768
– البنية التحتية الرقمية	-1.272	.393	1.758	.768
– المهارات الرقمية	-1.130	.393	1.868	.768
– الثقافة الرقمية	-.154	.393	.143	.768
البيئة الرقمية	-1.343	.393	2.628	.768

المصدر: من إعداد الطلبة بالإعتماد على مخرجات spss26

من خلال هذا الجدول أوضحت نتائج الاختبار مدى إتباع البيانات لتوزيع الطبيعي، حيث كانت قيمة معاملات الالتواء بالنسبة للمتغيرات الدراسة بمختلف أبعادها محصورة بين(**0.154- /-1.343**) وهي محصورة مابين [3- ، 3] أي البيانات لا تتبع انحرافاً كبيراً عن التوزيع الطبيعي وبالتالي فمتغيرات الدراسة تتبع التوزيع الطبيعي، ونتأكد من ذلك أيضا من خلال قيمة معاملات التفلطح التي كانت محصورة بين (**2.628/0.143**) أي هذه قيمة محصورة مـا بين [7- ،7] أي أن البيانات لا تحتوي على تفلطح وتحدب كبير يؤثر على نتائج التحليل مما يشير إلى أن البيانات في هذه الدراسة تتبع توزيعا طبيعيا بالتالي تحقق شروط إجراء التحليل الانحدار لضمان الوثوق بنتائجه والقدرة على مواصلة تحليل نموذج الدراسة اعتمادا على الأساليب الإحصائية المعلمية.

المبحث الثالث: نتائج دراسة تحليل الاستبيان

يعرض هذا المبحث النتائج التي تم التوصل إليها في الدراسة الميدانية من خلال التحليل الإحصائي للبيانات التي تم جمعها من استبيان الدراسة.

المطلب الأول: تحليل اجابات أفراد العينة.

سنتطرق لتحليل القسم الأول من الاستمارة، والذي يسمح لنا بالتعرف على بعض الخصائص المميزة لعينة الدراسة والمتمثلة في الجنس، العمر، ، سنوات الخبرة، رتبة الوظيفي، الكلية

أولا: توزيع عينة الدراسة حسب النوع الاجتماعي (الجنس).

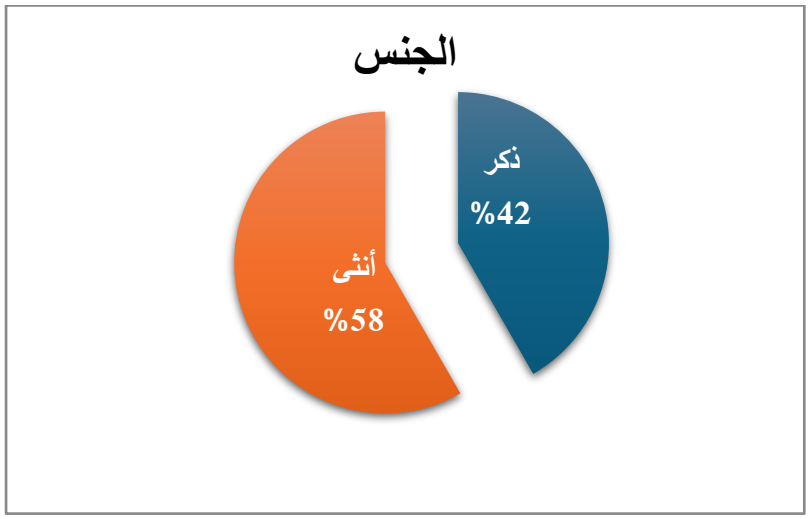
يتوزع أفراد عينة الدراسة حسب طبيعة جنسهم كما هو موضح في الجدول والشكل التاليين:

الجدول رقم(09): توزيع عينة الدراسة حسب النوع الاجتماعي.

النوع الإجتماعي	التكرارات	النسبة المئوية
ذكر	15	%41.7
أنثى	21	%58.3
المجموع	**36**	**%100**

المصدر: من إعداد الطلبة بالاعتماد على مخرجات SPSS V26

الشكل رقم(01): توزيع عينة الدراسة حسب النوع الاجتماعي



المصدر: مستخرج من EXCEL بالاعتماد على الجدول اعلاه.

يتضح من خلال معطيات الجدول والشكل البياني أعلاه أن نسبة الإناث ضمن عينة الدراسة بلغت 58%، في حين بلغت نسبة الذكور 42%. ويُظهر هذا التوزيع تفوقًا نسبيًا في عدد العاملين من الإناث على الذكور في جامعة محمد خيضر – بسكرة. ورغم هذا التفاوت، إلا أن الفارق يظل محدودًا، ما يعكس نوعًا من التوازن والتنوع في التمثيل بين الجنسين داخل المؤسسة. ويُعد

هذا التنوع في القوى العاملة مؤشرًا إيجابيًا، حيث يُمكن أن يسهم في تحسين الأداء التنظيمي، وتعزيز بيئة العمل من خلال تنوع الرؤى والخبرات، مما يدعم الإبداع والابتكار في معالجة المشكلات واتخاذ القرارات داخل الجامعة.

ثانيا: توزيع عينة الدراسة حسب الفئة العمرية.

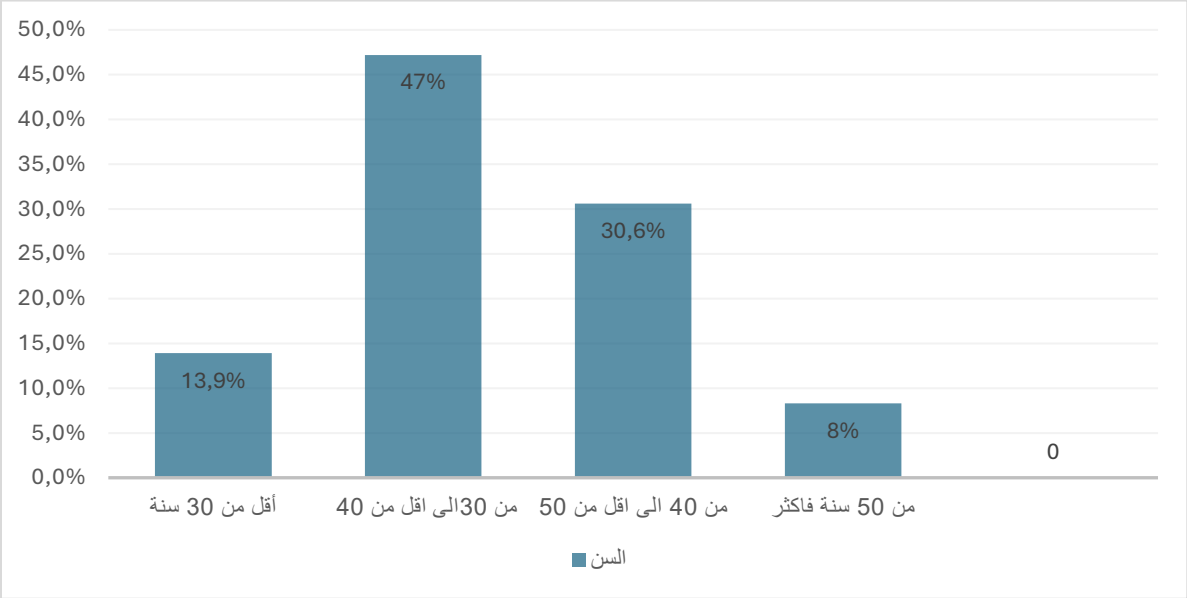
يتوزع أفراد عينة الدراسة حسب عمرهم كما هو موضح في الجدول والشكل التاليين:

جدول رقم(10): توزيع عينة الدراسة حسب متغير الفئة العمرية

العمر	التكرارات	النسبة المئوية
أقل من 30 سنة	05	%13.9
من 30الى اقل من 40	17	%47.2
من 40 الى اقل من 50	11	%30.6
من 50 سنة فاكثر	03	%8.3
المجموع	**36**	**100%**

المصدر: من إعداد الطلبة بالاعتماد على مخرجات SPSS V26

الشكل رقم(02): توزيع عينة الدراسة حسب متغير الفئة العمرية



المصدر: مستخرج من EXCELبالاعتماد على الجدول اعلاه

يتضح من معطيات الجدول أعلاه أن الغالبية العظمى من أفراد عينة الدراسة ينتمون إلى الفئة العمرية من **30إلى أقل من 40 سنة**، حيث بلغت نسبتهم **47.2%**، تليها الفئة العمرية من **40إلى أقل من 50 سنة** بنسبة **30.6%**. أما الفئتان العمريتان الأخريان، وهما فئة **أقل من 30 سنة** وفئة **50سنة فأكثر**، فقد سجلتا نسبًا أقل، بلغت **13.9%** و**8.2%** على التوالي. وتشير هذه النتائج إلى أن معظم أفراد العينة ينتمون إلى الفئة العمرية المتوسطة، وهي فئة غالبًا ما تمتاز بالتوازن بين الخبرة العملية والحيوية المهنية، مما قد ينعكس بشكل إيجابي على فهمهم لتحديات الأمن السيبراني واستيعابهم لمتطلبات البيئة الرقمية في المؤسسة الجامعية.

ثالثا: توزيع عينة الدراسة حسب سنوات الخبرة.

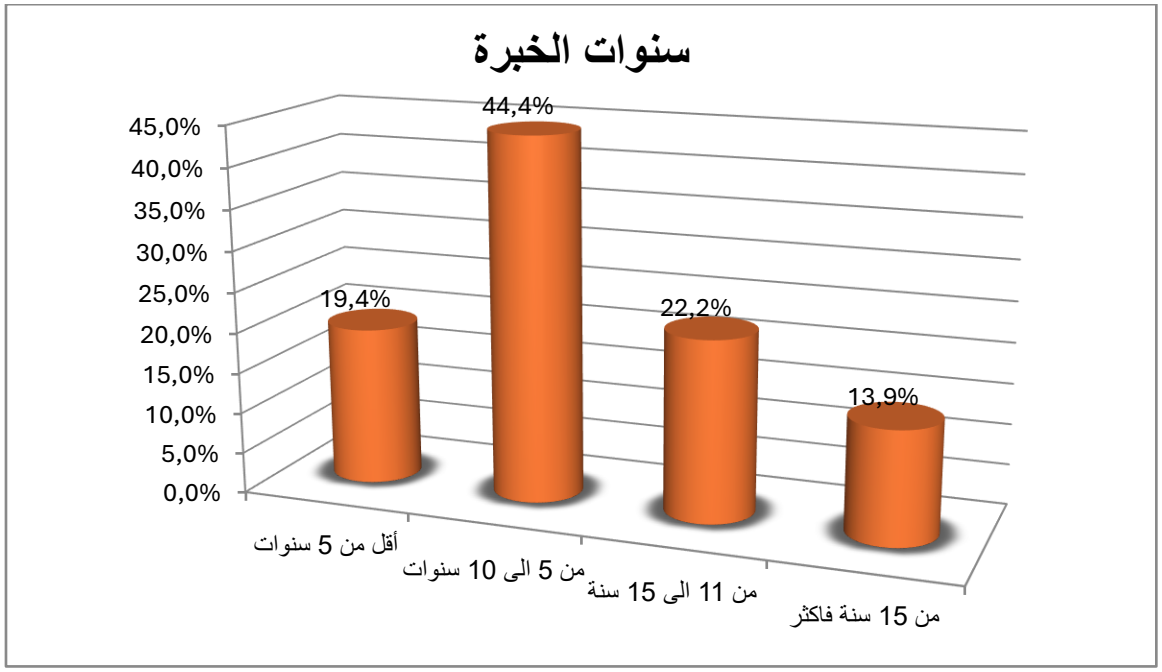
الجدول والشكل الآتيين يمثلان النتائج المتحصل عليها بخصوص توزيع عينة الدراسة حسب **سنوات الخبرة**

جدول رقم(11): توزيع عينة الدراسة حسب سنوات الخبرة.

سنوات الخبرة	التكرارات	النسبة المئوية
أقل من 5 سنوات	07	%19.4
من 5 الى 10 سنوات	16	%44.4
من 11 الى 15 سنة	08	%22.2
من 15 سنة فاكثر	05	%13.9
المجموع	**36**	**%100**

المصدر: من إعداد الطلبة بالاعتماد على مخرجات SPSS V26

الشكل رقم(03): توزيع أفراد عينة الدراسة حسب سنوات الخبرة



المصدر: مستخرج من EXCELبالاعتماد على الجدول اعلاه

يُظهر الجدول والشكل البياني أعلاه أن الفئة التي تحظى بأعلى نسبة من الخبرة المهنية ضمن عينة الدراسة هي الفئة التي تتراوح خبرتها بين **5إلى أقل من 10 سنوات**، حيث بلغت نسبتها **44.4%**، تليها فئة **11إلى أقل من 15 سنة** بنسبة **22.2%**، ثم فئة **أقل من 5 سنوات** بنسبة **19.4%**، وأخيرًا فئة **15سنة فأكثر** بنسبة.**13.9%** حيث تشير هذه النتائج إلى أن أغلب أفراد العينة يمتلكون خبرة تفوق الخمس سنوات، وهو ما يعكس وجود رصيد معرفي ومهني متراكم لدى الموظفين، يمكن أن يسهم بفعالية في تعزيز قدراتهم على التفاعل مع التحديات الرقمية، وفهم قضايا الأمن السيبراني، والاستفادة من تجاربهم في تحسين البيئة الرقمية داخل جامعة محمد خيضر – بسكرة.

رابعا: توزيع عينة الدراسة حسب المستوى الرتبة

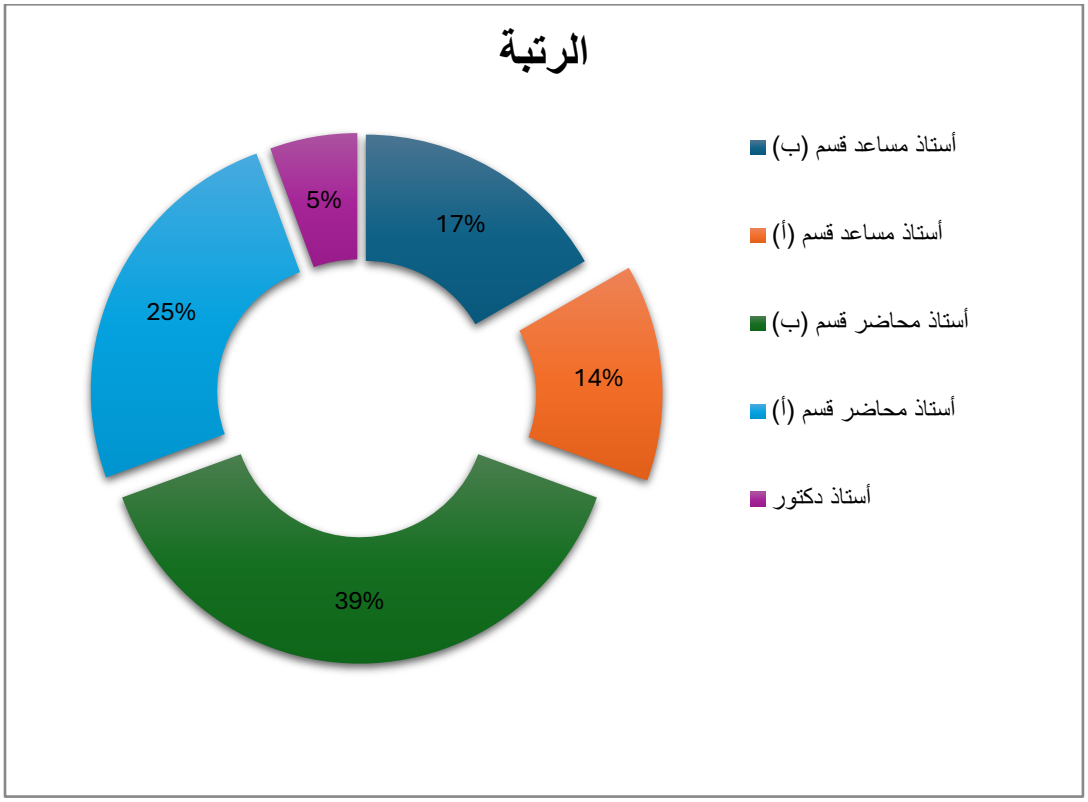
الجدول والشكل الآتيين يمثلان النتائج المتحصل عليها بخصوص توزيع عينة الدراسة حسب الرتبة.

الجدول رقم(12): توزيع عينة الدراسة حسب الرتبة

الرتبة	التكرارات	النسبة المئوية
أستاذ مساعد قسم (ب)	6	%16.7
أستاذ مساعد قسم (أ)	5	%13.9
أستاذ محاضر قسم (ب)	14	%38.9
أستاذ محاضر قسم (أ)	09	%25
أستاذ دكتور	2	5.6
المجمـــوع	**36**	**100%**

المصدر: من إعداد الطلبة بالاعتماد على مخرجات SPSS V26

الشكل رقم(04): توزيع عينة الدراسة حسب الرتبة



المصدر: مستخرج من EXCELبالاعتماد على الجدول اعلاه

يتضح من الجدول والشكل البياني السابق أن غالبية أفراد عينة الدراسة ينتمون إلى **رتبة أستاذ محاضر قسم (ب)** بنسبة بلغت **38.9%**، تليها **رتبة أستاذ محاضر قسم** (أ) بنسبة **25%**، ثم **أستاذ مساعد قسم (ب)** بنسبة **16.7%**، تليها **أستاذ مساعد قسم** (أ) بنسبة **13.9%**، وأخيرًا **أستاذ التعليم العالي** (**أستاذ دكتور**) بنسبة **5.6%** وتعتبر النسبة الأكبر ضمن رتب رتبة أستاذ

محاضر قسم (ب)، والتي تعكس بدورها واقع التوزيع الوظيفي للأساتذة في جامعة محمد خيضر – بسكرة. كما يشير هذا التنوع في الرتب العلمية إلى توافر مستويات مختلفة من الخبرة والمعرفة الأكاديمية، وهو ما يُمكن أن يثري نتائج الدراسة من خلال تعدد وجهات النظر وتفاوت درجات الفهم لقضايا الأمن السيبراني في البيئة الجامعية.

خامسا توزيع عينة الدراسة حسب الكلية.

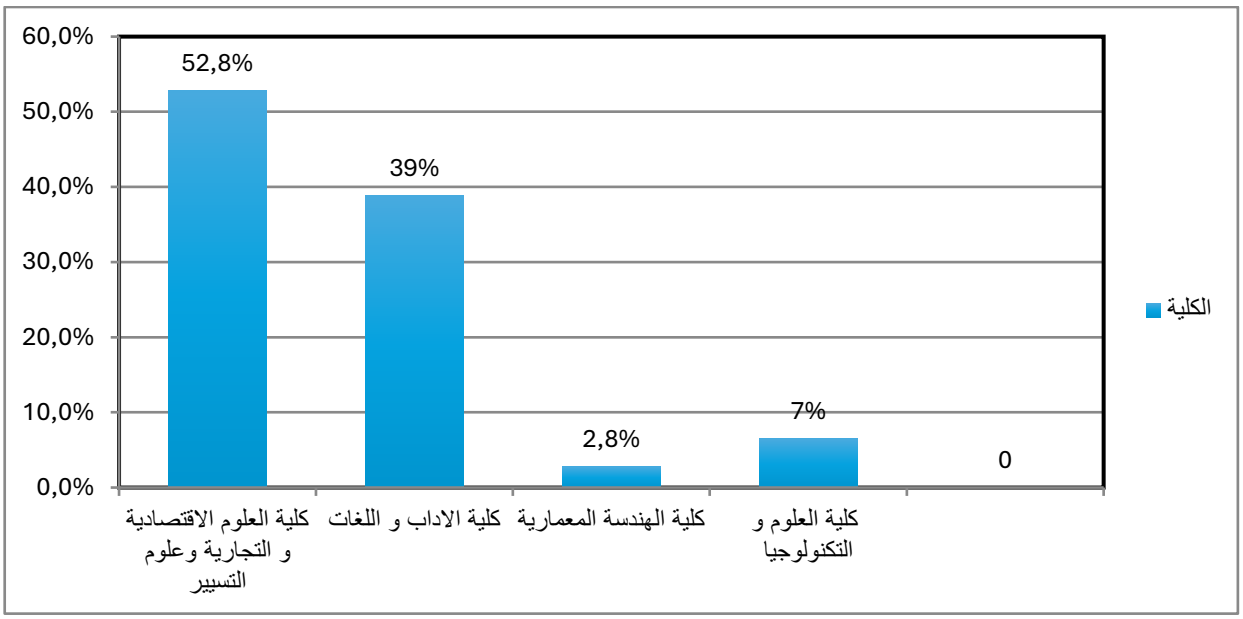
الجدول والشكل الآتيين يمثلان النتائج المتحصل عليها بخصوص توزيع عينة الدراسة حسب **الكلية**.

جدول رقم(13): توزيع عينة الدراسة حسب الكلية..

الكلية.	التكرارات	النسبة المئوية
كلية العلوم الاقتصادية و التجارية وعلوم التسيير	19	52.80%
كلية الآداب و اللغات	14	38.9%
كلية الهندسة المعمارية	1	2.8%
كلية العلوم و التكنولوجيا	2	6.5%
المجموع	**36**	**%100**

المصدر: من إعداد الطلبة بالاعتماد على مخرجات SPSS V26

الشكل رقم(05): توزيع أفراد عينة الدراسة حسب الكلية



المصدر: مستخرج من EXCELبالاعتماد على الجدول اعلاه

يتضح من خلال الجدول والشكل البياني أن أغلب أفراد العينة التي تم استرجاع استبياناتها ينتمون إلى **كلية العلوم الاقتصادية والتجارية وعلوم التسيير**، حيث بلغت نسبتهم **52.8%**، تليها **كلية الآداب** بنسبة **38.9%**.أما أقل نسب تمثل **كلية العلوم والتكنولوجيا** و**كلية الهندسة المعمارية**، فقد بلغت **6.5%** و **2.8%**على التوالي وتعتبر هذه النتائج إلى ما يبدو من تفرغ أساتذة

كليتي العلوم الاقتصادية والآداب وحرصهم على دعم الطلبة والمساهمة في إنجاح بحوثهم الأكاديمية، في حين قد يُفسر انخفاض تمثيل الكليتين الأخريين بانشغال الأساتذة أو طبيعة التزاماتهم الأكاديمية والإدارية، مما أثر على مشاركتهم في الدراسة.

المطلب الثاني: تحليل اتجاهات أفراد العينة نحو محاور الدراسة.

سيتم في هذا المطلب تحليل محاور الاستبيان بغرض الإجابة عن أسئلة الدراسة بناءًا على مخرجات البرنامج الإحصائي SPSS، حيث سيتم استخدام كل من قيمة المتوسط الحسابي والانحراف المعياري على مقياس ليكرت [1-5] لإجابات أفراد عينة الدراسة عن عبارات الاستبيان المتعلقة بمحور الأمن السيبراني والبيئة الرقمية.

الفرع الأول: تحليل بيانات محور الأمن السيبراني.

سنحلل نتائج عبارات محور المتغير الاول " الأمن السيبراني "، حيث تضمن هذا المحور(12) عبارات، وبعد تفريغ إجابات أفراد العينة، كانت النتائج موضحة في الجدول الموالي:

الجدول رقم(14): تحليل العبارات الخاصة بالمحور الاول

رقم العبارة	العبـــارت	المتوسط الحســابي	الانحراف المعيــاري	ترتيــب	اتجاه إجابات أفراد العينة
.1	توجد سياسة واضحة للأمن السيبراني في المؤسسة الجامعية.	3.64	.762	4	موافق
.2	تنظيم تدريبات للموظفين على أساسيات الأمن السيبراني بشكل منتظم.	3.69	.822	3	موافق
.3	استخدام برامج وتطبيقات موثوقة للحماية من الاختراقات والبرمجيات الخبيثة	3.44	1.206	10	موافق
.4	يُسمح فقط باستخدام البرمجيات المعتمدة على الأجهزة الجامعية.	3.89	1.008	1	موافق
.5	ايجاد اليات للإبلاغ عن التهديدات الأمنية الرقمية اتصال خارجية.	3.44	1.107	9	موافق
.6	يتم اتخاذ إجراءات فعلية بعد الإبلاغ عن التهديدات أو الحوادث الأمنية	3.25	1.273	12	محايد
.7	تعتقد أن الطلاب والموظفين بحاجة إلى برامج توعوية مستمرة حول الأمن السيبراني	3.53	1.028	6	موافق
.8	يتم تحديث الأنظمة التشغيلية والتطبيقات بانتظام داخل الجامعة	3.58	.967	5	موافق
.9	تعتقد أن الشبكة الداخلية للجامعة آمنة بما فيه الكفاية	3.50	1.159	7	موافق

.10	**تترك أجهزتك مفتوحة أو غير مؤمّنة عند الابتعاد عنها**	3.42	1.131	**11**	**موافق**
.11	**تقوم بفحص الروابط أو المرفقات قبل فتحها عبر البريد الإلكتروني**	3.44	.909	**8**	**موافق**
.12	**تستخدم كلمات مرور قوية ومختلفة لحساباتك الجامعية.**	3.86	.867	**2**	**موافق**
	الأمن السيبراني	3.5579	.62925		**موافق**

المصدر: من إعداد الطلبة باستخدام مخرجات spss 26

يتضح من الجدول أعلاه أن اتجاهات مفردات عينة الدراسة قد أظهرت ميولًا إيجابية نحو الموافقة على عبارات محور **الأمن السيبراني**، حيث بلغ المتوسط الحسابي الكلي لهذا المحور (**3.5579**)، مصحوبًا بانحراف معياري قدره .(**0.62925**)وتشير هذه القيم إلى وجود تفاوت متوسط في آراء أفراد العينة، مما يعكس اختلافًا معتدلًا في مستوى الإدراك والرضا، إلا أن الاتجاه العام يظل إيجابيًا، بما يفيد أن غالبية الأساتذة يرون أن جامعة محمد خيضر – بسكرة تولي اهتمامًا ملحوظًا بمسائل الأمن السيبراني.

وقد جاءت العبارو رقم (04): "**يسمح فقط باستخدام البرمجيات المعتمدة على الأجهزة الجامعية**"، كأعلى العبارات من حيث درجة الموافقة، بمتوسط حسابي بلغ (**3.89**)، وهو ما يعكس وجود سياسة واضحة لدى الجامعة بشأن ضبط استخدام البرمجيات على أجهزتها، بما يحد من مخاطر الاختراقات الرقمية أو البرمجيات الخبيثة، ويعد هذا مؤشرًا إيجابيًا على مستوى الوعي المؤسسي، في المقابل، كانت العبارة (06) "**تعتقد أن الطلاب والموظفين بحاجة إلى برامج توعوية مستمرة حول الأمن السيبراني**"، هي الأقل من حيث درجة الموافقة بالحيادية، بمتوسط حسابي قدره (**3.25**) وتشير هذه النتيجة إلى وجود قدر من التحفظ أو الحياد بين أفراد العينة حول مدى كفاية برامج التوعية الحالية، وهو ما يُمكن تفسيره إما بوجود نقص فعلي في هذا الجانب، أو باختلاف وجهات النظر حول فعالية التوعية المقدمة داخل الجامعة.

وبناءً على ما سبق، يمكن القول إن جامعة محمد خيضر – بسكرة تُبدي اهتمامًا ملحوظًا بالأمن السيبراني، ويُنظر إلى هذا الاهتمام بإيجابية من قبل الأساتذة، لا سيما فيما يخص الإجراءات التقنية الوقائية. ومع ذلك، فإن جانب التوعية والتثقيف المستمر ما يزال يتطلب مزيدًا من التعزيز والتطوير لضمان بيئة رقمية آمنة ومستدامة على كافة المستويات.

الفرع الثاني: تحليل بيانات محور أبعاد البيئة الرقمية.

من خلال هذا الفرع سنحلل نتائج عبارات أبعاد محور البيئة الرقمية وذلك بالاستعانة بكل من المتوسط الحسابي والانحراف المعياري، والترتيب حسب درجة الأهمية واتجاه آراء أفراد العينة لكل بعد من أبعاد هذا المحور، كما هو موضح في الجدول الموالي:

أولا: البعد الأول (البنية التحتية الرقمية)

تضمن هذا البعد 06 عبارات، والجدول الموالي يوضح إجابات أفراد العينة حول عبارات هذا البعد.

الجدول رقم(15): تحليل العبارات الخاصة بالبعد الاول.

رقم العبارة	العبـــارت	المتوسط الحســابي	الانحـراف المعيــاري	الترتيــب	اتجاه إجابات أفراد العينة
.1	توافر شبكة انترنت مستقرة وسريعة في بيئة العمل	3.06	1.218	5	محايد
.2	اجراء تحديثات للأجهزة الرقمية والبرمجيات المستخدمة بشكل دوري	3.42	1.052	2	موافق
.3	توفير خوادم امنة ومساحات تخزين سحابية موثوقة لحفظ البيانات	3.69	.980	1	موافق
.4	صيانة البنية التحتية الرقمية بانتظام لضمان الاستمرارية	3.28	1.256	4	محايد
.5	تخصيص ميزانيات دورية لتطوير البنية التحتية التقنية	2.97	.971	6	محايد
.6	يتم فحص أمان الخوادم بشكل منتظم لحماية المعلومات من الاختراقات	3.33	1.121	3	محايد
	البنية التحتية الرقمية	3.2917	.78414		محايد

المصدر: من إعداد الطلبة باستخدام مخرجات spss26

من خلال بيانات الجدول السابق، يتبين أن اتجاهات مفردات عينة الدراسة جاءت محايدة بشكل عام فيما يتعلق بـ بُعد **البنية التحتية الرقمية**، حيث بلغ المتوسط الحسابي لهذا البعد (**3.2917**)، مصحوبًا بانحراف معياري قدره .(**0.78414**)وتشير هذه النتائج إلى أن آراء الأساتذة تفاوتت بدرجة طفيفة، ما يعكس وجود درجة محدودة من التباين في وجهات النظر حول مدى تطور وتوفر البنية التحتية الرقمية داخل الجامعة. ويُظهر الانحراف المعياري أن الاختلافات في الإجابات ليست كبيرة، لكنها قائمة إلى حد ما، وهو ما يُفسر الاتجاه العام نحو الحياد.

وفيما يتعلق بترتيب العبارات، فقد جاءت العبارة رقم" :(03) **توفير خوادم آمنة ومساحات تخزين سحابية موثوقة لحفظ البيانات** "في صدارة العبارات من حيث درجة الموافقة، بمتوسط حسابي قدره (**3.69**)، ما يشير إلى وجود إدراك إيجابي بين أفراد العينة حول جهود الجامعة في تأمين وتوفير البنية التحتية الأساسية اللازمة لحماية البيانات.في المقابل، سجلت العبارة رقم :(05) "**تخصيص ميزانيات دورية لتطوير البنية التحتية التقنية**" أدنى متوسط حسابي بلغ (**2.97**)، وهو ما يعكس ضعف القناعة لدى

الأساتذة بوجود استثمار منتظم ومخطط في هذا الجانب الحيوي .ويُفهم من ذلك أن هناك نوعًا من التردد أو الشك بشأن التزام المؤسسة بتخصيص موارد مالية مستمرة لتحسين البنية التحتية الرقمية، وهو عنصر أساسي لتحقيق التحول الرقمي المستدام.

بشكل عام، يُمكن القول إن تقييم أفراد العينة لبُعد البنية التحتية الرقمية في جامعة محمد خيضر – بسكرة جاء في المستوى المتوسط، بما يعكس توجّهًا حياديًا نحو مدى تطورها وكفاءتها. وهذا يشير إلى أن الجامعة قد تكون قد أحرزت تقدمًا في بعض الجوانب التقنية، مثل توفير الخوادم والتخزين السحابي، لكنها بحاجة إلى تعزيز جهودها في مجالات التخطيط المالي والتطوير المستدام للبنية التحتية الرقمية من أجل تحسين الأداء الرقمي ورفع مستوى الكفاءة التشغيلية.

ثـانيـا: البعد الثـاني (المهارات الرقمية)

يتضمن هذا البعد 05 عبارات، وبعد تفريغ إجابات أفراد العينة كانت النتائج موضحة في الجدول كالآتي:

الجدول رقم(16): تحليل العبارات الخاصة بالبعد الثاني.

رقم العبارة	العبـــارت	المتوسط الحســابي	الانحراف المعيــاري	ترتيـــب	اتجاهإجابات أفراد العينة
.7	أمتلك القدرة على استخدام البرمجيات الأساسية في بيئة العمل	3.56	.877	3	موافق
.8	أستطيع التعامل مع الأنظمة الرقمية المستخدمة بكفاءة والمنصات التعليمية	3.81	.980	2	موافق
.9	أتمكن من حماية بياناتي الشخصية والمهنية الكترونيا	3.33	1.069	4	محايد
.10	تمكن من التعلم الذاتي عبر الأنترنت لتعزيز مهاراتي الرقمية	3.03	1.134	5	محايد
.11	أطور مهاراتي الرقمية من خلال التدريب الذاتي أو الرسمي	3.83	.697	1	موافق
	المهارات الرقمية	3.5111	.65106		موافق

المصدر: من إعداد الطالبة باستخدام مخرجات spss26

يتضح من خلال بيانات الجدول السابق أن اتجاهات مفردات عينة الدراسة أظهرت توافقًا عامًا إيجابيًا نحو بُعد المهارات الرقمية، حيث بلغ المتوسط الحسابي (**3.5111**)، مصحوبًا بانحراف معياري قدره (**0.65106**)، ما يدل على وجود درجة معتدلة من التجانس في آراء أفراد العينة بشأن أهمية المهارات الرقمية ودورها في فهم البيئة الرقمية. وتُبرز هذه النتائج أن الغالبية العظمى من الأساتذة المشاركين في الدراسة يرون أن المهارات الرقمية تمثل عنصرًا محوريًا في التكيف مع متطلبات البيئة الرقمية وتعزيز كفاءة الأداء الأكاديمي والإداري في الجامعة. وفي تفصيل العبارات، سجلت العبارة رقم" :(11) **أطور مهاراتي الرقمية من خلال التدريب الذاتي أو الرسمي** "أعلى متوسط حسابي بلغ (**3.83**)، ما يعكس توافقًا واضحًا بين الأساتذة حول أهمية الاستثمار في تنمية قدراتهم الرقمية بشكل فردي أو عبر برامج التدريب الرسمي، ويُظهر كذلك وجود ثقافة ذاتية للتعلم المستمر في أوساط الكادر الأكاديمي، في

المقابل، جاءت العبارة رقم" :(10) **أتمكن من التعلم الذاتي عبر الإنترنت لتعزيز مهاراتي الرقمية** "بأقل متوسط حسابي بلغ (**3.03**)، مما يشير إلى تفاوت في مدى الاعتماد على التعلم الذاتي الإلكتروني بين أفراد العينة، أو ربما وجود تحديات تحول دون الاستفادة الكاملة من الموارد الرقمية المتاحة على الإنترنت، كقلة التوجيه أو ضعف البنية التحتية ذات الصلة.

بصورة عامة، يُمكن القول إن المتوسط الحسابي المرتفع نسبيًا لهذا البُعد يعكس مستوى جيدًا من الاطلاع والتمكن من المهارات الرقمية لدى الأساتذة بجامعة محمد خيضر – بسكرة، وهو ما يشكل دعامة أساسية لتفعيل الممارسات الرقمية وتحقيق التحول نحو بيئة جامعية رقمية متكاملة.

ثالثا: البعد الثالث (الثقافة الرقمية)

يتضمن هذا البعد05 عبارات، وبعد تفريغ إجابات أفراد العينة كانت النتائج موضحة في الجدول كالآتي:

الجدول رقم(17): تحليل العبارات الخاصة بالبعد الثالث

رقم العبارة	العبـــارت	المتوسط الحســابي	الانحـراف المعيــاري	ترتيــب	اتجاه إجابات أفراد العينة
.12	تدرك أهمية السلوك الرقمي المسؤول عند استخدام الأنترنت	3.61	.766	4	موافق
.13	تلتزم بالقوانين والأنظمة المتعلقة بالاستخدام الرقمة	4.00	.793	3	موافق
.14	ادارة الجامعة تتعامل بجدية مع مشكلات الأمن الرقمي	3.25	1.052	5	محايد
.15	تحرص على احترام خصوصية الاخرين في البيئات الرقمية	4.06	.630	1	موافق
.16	تشعر بالثقة عند استخدام البريد الالكتروني الجامعي	4.00	.632	2	موافق
	الثقافة الرقمية	3.7833	.39821		موافق
	البيئة الرقمية	3.5287	.49571		موافق

المصدر: من إعداد الطالبة باستخدام مخرجات spss26

يُظهر الجدول السابق أن اتجاهات مفردات عينة الدراسة جاءت عامةً إيجابية نحو بُعد الثقافة الرقمية، حيث بلغ المتوسط الحسابي (**3.7833**)، وهو معدل مرتفع نسبيًا، مما يعكس وجود وعي متقدم وثقافة رقمية متجذّرة لدى أفراد العينة، كما أن الانحراف المعياري البالغ (**0.39821**) يدل على وجود تباين ضعيف في الآراء، ما يعني تقارب وجهات النظر حول هذا البعد.

وقد سجلت العبارة رقم" :(15) **أحرص على احترام خصوصية الآخرين في البيئات الرقمية** "أعلى متوسط حسابي قدره (4.06)، ما يعكس اتفاقًا قوياً بين أفراد العينة على أهمية احترام الخصوصية في الفضاء الرقمي، وهو مؤشر إيجابي على التزامهم بالقيم الأخلاقية والسلوكية في التعامل الرقمي، وفي المقابل، جاءت العبارة رقم" :(**14**) **إدارة الجامعة تتعامل بجدية مع مشكلات الأمن الرقمي** " بأقل متوسط حسابي بلغ (**3.25**)، وهو ما يشير إلى وجود بعض التحفظات أو الشكوك حول فاعلية الإدارة في معالجة التحديات الرقمية، وقد يُعزى ذلك إلى نقص في الشفافية أو ضعف التواصل المؤسسي بشأن الإجراءات الأمنية المتخذة.

وبناءً على ما سبق، يُمكن القول إن المتوسط المرتفع لبُعد الثقافة الرقمية يعكس تفوقًا ملحوظًا في الجانب القيمي والمعرفي المرتبط باستخدام الوسائط الرقمية داخل الجامعة، وهو ما يُعدّ مؤشراً إيجابياً على جاهزية الأساتذة لتبني السلوكيات المثلى في البيئة الرقمية.

أما فيما يخص محور البيئة الرقمية بشكل عام، فقد أظهرت نتائج الدراسة اتجاهاً عاماً نحو الموافقة، حيث بلغ المتوسط الحسابي (**3.5287**)بانحراف معياري قدره (**0.49571**)، ما يشير إلى وجود تشتت طفيف في الآراء، ويعكس رضىً عاماً بين أفراد العينة حول الجهود المبذولة من طرف الجامعة في تحسين بيئتها الرقمية، سواء من حيث البنية التحتية أو الثقافة أو المهارات الرقمية. كما يشير ذلك إلى أن الجامعة تسير في الاتجاه الصحيح نحو تعزيز بيئة رقمية فعالة ومستدامة، تواكب التغيرات التكنولوجية وتستجيب لتطلعات المستخدمين

المطلب الثالث: اختبار الفرضيات.

في هذا المطلب سنتطرق إلى تحليل الانحدار البسيط لاختبار الفرضيات الرئيسة والفرعية للدراسة، والهدف منه هو التحقق من خطية العلاقة بين المتغير المستقل و المتغير التابع.

الفرع الاول: اختبار الانحدار البسيط للاستبيان.

أولا: تحليل الانحدار البسيط بين الامن السيبراني والبنية التحتية.

بإستخدم اختبار تحليل الانحدار البسيط لتحقق من وجود دور وأثر بين **الامن السيبراني والبنية التحتية الرقمية في جامعة محمد خيضر بسكرة**، كانت النتائج كما هي موضح في الجدول الموالي:

الجدول رقم(18): يوضح نتائج تحليل الانحدار البسيط بين الامن السيبراني والبنية التحتية الرقمية.

الامن السيبراني						
البنية التحتية الرقمية	معامل الإرتباط R	معامل التحديد R^2	مستوى الدلالة Sig	قيمةT المحسوبة	قيمةF المحسوبة	معامل الإنحدارB
	0.883	0.774	0.000	10.983	120.627	0.709

المصدر:من إعداد الطلبة باستخدام مخرجات spss 26

من خلال نتائج الواردة في الجدول اعلاه يتضح أن:

- **معامل الإرتباطR**: من خلال قيمة الارتباط المقدرة ب(0.883)، وقيمة مستوى المعنوية اقل من 0.05 يدل على وجود علاقة قوية بين **الامن السيبراني والبنية التحتية**.
- **معامل التحديد R^2**: من خلال معامل التحديد الذي قدر ب(0.774)، يتضح أن العمل الامن السيبراني يحدث تغير في البنية التحتية الرقمية بنسبة 77 %.
- **معنوية التأثير قيمة T المحسوبة**: تشير قيمة T المحسوبة والمقدرة ب(10.983)، الأكبر من القيمة الجدولية إلى وجود تأثير لمحور الامن السيبراني على البنية التحتية الرقمية.

- **جودة النموذج قيمةF المحسوبة**: تشير قيمة F المحسوبة والتي تقدر ب(120.627)، إلى جودة نموذج العلاقة بين الامن السيبراني والبنية التحتية الرقمية.
- **معامل الانحدار B (معامل التأثير)**: تشير قيمة معامل التأثير والمقدرة ب(0.709)، إلى أنه كلما زادت الجهود المبذولة لانجاح **الامن السيبراني** بوحدة واحدة يعقبها زيادة في تحسين **البنية التحتية الرقمية** بنسبة 70%.

ثانيا: تحليل الانحدار البسيط بين الامن السيبراني والمهارات الرقمية.

بإستخدم اختبار تحليل الانحدار البسيط لتحقيق وجود دور وأثر بين **الامن السيبراني والمهارات الرقمية في جامعة محمد خيضر بسكرة** ، كانت النتائج كما هو موضح في الجدول الموالي:

ال**جدول رقم(19): يوضح نتائج تحليل الانحدار البسيط بين بين الامن السيبراني والمهارات الرقمية.**

الامن السيبراني						
المهارات الرقمية.	معامل الإرتباط R	معامل التحديد R^2	مستوى الدلالة Sig	قيمةT المحسوبة	قيمةF المحسوبة	معامل الإنحدارB
	0.742	0.550	0.000	6.448	41.578	0.717

المصدر:من إعداد الطلبة باستخدام مخرجات spss26

من خلال نتائج الواردة في الجدول اعلاه يتضح أن:

- **معامل الإرتباطR** : من خلال قيمة الارتباط المقدرة ب(0.742)، وقيمة مستوى المعنوية اقل من 0.05 يدل على وجود علاقة قوية بين **الامن السيبراني والمهارات الرقمية**.
- **معامل التحديد R^2** : من خلال معامل التحديد الذي قدر ب(0.550)، يتضح أن **الامن السيبراني** يغير من **المهارات الرقمية** بنسبة 55%.
- **معنوية التأثير قيمة T المحسوبة**: تشير قيمة T المحسوبة والمقدرة ب(6.448)، الأكبر من القيمة الجدولية إلى وجود تاثير بين **الامن السيبراني والمهارات الرقمية**.
- **جودة النموذج قيمةF المحسوبة**: تشير قيمة F المحسوبة والتي تقدر ب(41.578)، إلى جودة نموذج العلاقة بين **الامن السيبراني والمهارات الرقمية**.
- **معامل الانحدار B (معامل التأثير)**: تشير قيمة معامل التأثير والمقدرة ب(0.717)، إلى أنه كلما زادت الجهود المبذولة لانجاح **الامن السيبراني** بوحدة واحدة يعقبها زيادة في تحسين **المهارات الرقمية** بنسبة 71%.

ثـالثـا: تحليل الانحدار البسيط بين الامن السيبراني والثقافة الرقمية.

بإستخدم اختبار تحليل الانحدار البسيط لتحقيق وجود دور وأثر بين **الامن السيبراني والثقافة الرقمية في جامعة محمد خيضر بسكرة**، كانت النتائج كما هو موضح في الجدول الموالي:

الجدول رقم(20): يوضح نتائج تحليل الانحدار البسيط بين الامن السيبراني والثقافة الرقمية.

الامن السيبراني						
الثقافة الرقمية.	معـامـل الإرتبـاط R	مـعامـل التحديـد R^2	مستوى الدلالة Sig	قيمةT المحسوبـة	قيمةF المحسوبـة	معامـل الإنحدارB
	0.226	0.051	0.184	1.355	1.835	0.184

المصدر: من إعداد الطلبة باستخدام مخرجات spss 26

من خلال نتائج الواردة في الجدول اعلاه يتضح أن:

- **معامل الإرتباط R**: من خلال قيمة الارتباط المقدرة ب(0.226)، وقيمة مستوى المعنوية أكبر من 0.05 مما يدل على عدم وجود علاقة بين **الامن السيبراني والثقافة الرقمية**.
- **معامل التحديد R^2** : من خلال معامل التحديد الذي قدر ب(0.051)، يتضح أن وجود **الامن السيبراني** يساهم في احداث تغير **الثقافة الرقمية** بنسبة 5 %.
- **معنوية التأثير قيمة T المحسوبة**: تشير قيمة T المحسوبة والمقدرة ب(1.355)، الاقل من القيمة الجدولية إلى عدم وجود تاثير بين **الامن السيبراني والثقافة الرقمية**.
- **جودة النموذج قيمةF المحسوبة**: تشير قيمة F المحسوبة والتي تقدر ب(1.835)، إلى عدم جودة نموذج العلاقة أي غير معنوي إحصائيًا، بين **الامن السيبراني والثقافة الرقمية**.
- **معامل الانحدار B (معامل التأثير)**: تشير قيمة معامل التأثير والمقدرة ب(0.184)، إلى أنه كلما زادت الجهود المبذولة لتطبيق **الامن السيبراني**. بوحدة واحدة يعقبها زيادة في تحسين **الثقافة الرقمية** بنسبة 18%.

رابعا : تحليل الانحدار البسيط بين الامن السيبراني والبيئة الرقمية.

بإستخدم اختبار تحليل الانحدار البسيط لتحقق من وجود دور وأثر بين **الامن السيبراني والبيئة الرقمية في جامعة محمد خيضر بسكرة**، كانت النتائج كما هي موضح في الجدول الموالي:

الجدول رقم(21): يوضح نتائج تحليل الانحدار البسيط بين الامن السيبراني والبيئة الرقمية.

الامن السيبراني						
البيئة الرقمية	معامل الإرتباط R	معامل التحديد R^2	مستوى الدلالة Sig	قيمةT المحسوبة	قيمةF المحسوبة	معامل الإنحدارB
	0.851	0.724	0.000	9.450	89.310	1.080

المصدر: من إعداد الطلبة باستخدام مخرجات spss26

من خلال نتائج الواردة في الجدول اعلاه يتضح أن:

- **معامل الإرتباطR** : من خلال قيمة الارتباط المقدرة ب(0.851)، وقيمة مستوى المعنوية أقل من 0.05 مما يدل على وجود علاقة قوية بين **الامن السيبراني والبيئة الرقمية**.
- **معامل التحديد R^2** : من خلال معامل التحديد الذي قدر ب(0.724)، يتضح أن **الامن السيبراني** يساهم في تغيير **البيئة الرقمية** بنسبة 72%.
- **معنوية التأثير قيمة T المحسوبة**: تشير قيمة T المحسوبة والمقدرة ب(9.450)، الأكبر من القيمة الجدولية والدالة الإحصائية عند مستوى دلالة (0.000) إلى وجود تأثير **الامن السيبراني والبيئة الرقمية**.
- **جودة النموذج قيمةF المحسوبة**: تشير قيمة F المحسوبة والتي تقدر ب(89.310)، إلى جودة نموذج العلاقة بين **الامن السيبراني والبيئة الرقمية**.
- **معامل الانحدار B (معامل التأثير)**: تشير قيمة معامل التأثير والمقدرة ب(1.080)، إلى أنه كلما زادت الجهود المبذولة لتطبيق **الامن السيبراني**.بوحدة واحدة يعقبها زيادة في تحسين **البيئة الرقمية** بقيمة 1.080.

الفرع الثاني: اختبار فرضيات دراسة.

بعد تحليل العلاقة بين كل من **الامن السيبراني والبيئة الرقمية وابعادها** بجامعة محمد خيضر بسكرة كانت العلاقة إيجابية عند معنوية اختبار الفصل (0.05) والتي كانت مدخل لمناقشة الفرضيات واختبارها.

تم استخدام تحليل الارتباط وتحليل الانحدار البسيط في اختبار الفرضية الرئيسية و الفرعية التابعة لها، للتأكد من صلاحية النموذج، وقد اعتمدت قاعدة القرارات التالية:

- الفرضية الصفريةH0 : هناك دور ذو دلالة احصائية للامن السيبراني على البيئة الرقمية بجامعة محمد خيضر بسكرة
- الفرضية الصفريةH1 : ليس هناك دور ذو دلالة احصائية للامن السيبراني على البيئة الرقمية بجامعة محمد خيضر بسكرة
- قبول الفرضية الصفرية H0 : إذا كانت قيمة مستوى الدلالة المعنوية أقل من (0.05).

- قبول الفرضية H1 : إذا كانت قيمة مستوى الدلالة المعنوية أكبر من (0.05).

من أجل إختبار الفرضية الرئيسية ومعرفة مدى قبولها أو رفضها، علينا أولا أن نختبر الفرضيات الفرعية.

أولا: اختبار الفرضية الفرعية الأولى

" هناك دور ذو دلالة احصائية للامن السيبراني في تحسين البنية التحتية الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)."

أظهرت نتائج التحليل الإحصائي الموضحة بالجداول السابقة أن مستوى الدلالة المعنوية كانت أقل من 0.05 مما يعني قبول الفرضية الصفرية H0 ورفض الفرضية البديلة H1 والذي ينص على ان **هناك دور ذو دلالة احصائية للامن السيبراني في تحسين البنية التحتية الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)."** وهذا ما يعني صحة الفرضية الفرعية الأولى.

ثانيا: اختبار الفرضية الفرعية الثانية

" هناك دور ذو دلالة احصائية للامن السيبراني في تحسين المهارات الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)."

أظهرت نتائج التحليل الإحصائي الموضحة بالجداول السابقة أن مستوى الدلالة المعنوية كانت أقل من 0.05 مما يعني قبول الفرضية الصفرية H0 ورفض الفرضية البديلة H1 والذي ينص على ان هناك **هناك دور ذو دلالة احصائية للامن السيبراني في تحسين المهارات الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)**. وهذا ما يعني صحة الفرضية الفرعية الثانية.

ثالثا: اختبار الفرضية الفرعية الثالثة

" " هناك دور ذو دلالة احصائية للامن السيبراني في تحسين الثقافة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)."

أظهرت نتائج التحليل الإحصائي الموضحة بالجداول السابقة أن مستوى الدلالة المعنوية كانت أكبر من 0.05 مما يعني رفض الفرضية الصفرية H0 و قبول الفرضية البديلة H1 والذي ينص على ان **ليس هناك دور ذو دلالة احصائية للامن السيبراني في تحسين الثقافة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)**، وهذا ما يعني عدم صحة الفرضية الفرعية الثالثة.

رابعا: اختبار الفرضية الرئيسية

"هناك دور ذو دلالة احصائية للامن السيبراني في تحسين البيئة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)."

أظهرت نتائج التحليل الإحصائي الموضحة بالجداول السابقة أن مستوى الدلالة المعنوية كانت أقل من 0.05 مما يعني قبول الفرضية الصفرية H0 ورفض الفرضية البديلة H1 والذي ينص على ان " **هناك دور ذو دلالة احصائية للامن السيبراني في تحسين البيئة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)**. وهذا ما يعني صحة الفرضية الرئيسية.

خلاصـة الفصل:

في هذا الفصل، تم تقديم لمحة عامة عن **جامعة محمد خيضر – بسكرة**، باعتبارها البيئة التي أجريت فيها الدراسة الميدانية. وقد اعتمدنا في إنجاز هذا العمل على **أداة** الاستبانة، التي وُزعت على مجموعة من موظفي الجامعة، واحتوت على محاور أساسية تمثلت في :الأمن السيبراني والبيئة الرقمية، بهدف الإجابة عن إشكالية البحث التالية: "**ما هو دور الأمن السيبراني في تحسين البيئة الرقمية بجامعة محمد خيضر – بسكرة؟**"

بعد استرجاع الاستبانات، تم تفريغ البيانات وتحليلها باستخدام مجموعة من الأساليب الإحصائية، مثل :النسب المئوية، المتوسط الحسابي، الانحراف المعياري، واختبار ألفا كرونباخ لقياس الثبات.

وقد تم عرض وتحليل وتفسير النتائج، بالإضافة إلى اختبار الفرضيات، حيث توصلنا إلى عدد من النتائج، كان من أبرزها: وجود علاقة ذات دلالة إحصائية بين الأمن السيبراني وتحسين البيئة الرقمية في جامعة محمد خيضر – بسكرة، وذلك عند مستوى دلالة.(0.05)

كما أظهرت النتائج، عند تحليل أثر كل محور من محاور الاستبيان بشكل مستقل، أن الأمن السيبراني يؤثر بشكل مباشر في مستوى امتلاك وتحسين المهارات الرقمية لدى أفراد عينة الدراسة .وقد ثبت أن هذا التأثير ذو دلالة إحصائية أيضًا عند مستوى معنوية($\alpha = 0.05$)

الخاتمـــة

الخاتمة

في ضوء ما توصلنا إليه من خلال الدراسة النظرية والميدانية حول موضوع "دور الأمن السيبراني في تحسين البيئة الرقمية"، وتطبيقا على جامعة محمد خيضر بسكرة، تبيّن أن الأمن السيبراني يعد عنصرا أساسيا ومحوريا في تعزيز فعالية التحول الرقمي وضمان استقراره داخل المؤسسات الجامعية فمع تنامي الاعتماد على النظم الرقمية في مختلف جوانب العمل الجامعي، من التدريس والتعلم، إلى البحث العلمي والإدارة الإلكترونية، أصبحت حماية هذه الأنظمة من التهديدات السيبرانية أمرا لا غنى عنه.

ولقد أظهرت نتائج الدراسة أن وجود سياسات وإجراءات أمنية رقمية فعالة داخل الجامعة ساهم في تقليص المخاطر المرتبطة بالهجمات الإلكترونية والاختراقات، مما ساعد في توفير بيئة معلوماتية آمنة تحفظ سرية البيانات وتحمي خصوصية المستخدمين. كما أن تعزيز الوعي الأمني لدى الأساتذة والعاملين والطلبة، سواء من خلال برامج تدريبية أو ممارسات وقائية، لعب دورا مهما في دعم هذا التوجه، ومن جهة أخرى، فإن تحسن البيئة الرقمية بالجامعة لم يكن ليتحقق لولا التكامل الواضح بين المهارات الرقمية المكتسبة من طرف الموارد البشرية، والبنية التحتية التقنية التي توفرها الجامعة. وقد ساعد هذا التفاعل في بناء مناخ تكنولوجي يدعم الابتكار، ويسهل من الأداء اليومي للأفراد، ويرتقي بجودة الخدمات المقدمة سواء على المستوى الأكاديمي أو الإداري.

كما أن هذا الاهتمام المتزايد بالأمن السيبراني انعكس بشكل إيجابي على سلوك الأفراد داخل المؤسسة، حيث لوحظ وجود ثقافة رقمية ناضجة تعزز من احترام الخصوصية الرقمية، وتحث على الاستخدام المسؤول للتقنيات. وبالتالي، يمكن القول إن جامعة محمد خيضر بسكرة تسير في اتجاه تعزيز بيئتها الرقمية بشكل متوازن، من خلال الجمع بين الحماية الأمنية والتمكين التكنولوجي، بما يخدم تطلعاتها نحو جامعة ذكية وآمنة.

وفي المجمل، تبرز هذه الدراسة أهمية إدماج الأمن السيبراني كعنصر أساسي ضمن استراتيجيات التحول الرقمي في المؤسسات، باعتباره شرطًا مسبقًا لنجاح أي تجربة رقمية، وضمانا لاستمراريتها وفعاليتها في ظل التحديات الرقمية المتزايدة.

I. النتائج النظرية

. من خلال الاستعراض النظري لموضوع الأمن السيبراني والبيئة الرقمية، تم التوصل إلى جملة من النتائج، من أبرزها:

1. الأمن السيبراني ركيزة أساسية للتحول الرقمي حيث يمثل الضمانة الأساسية لحماية النظم الإلكترونية والبنية التحتية الرقمية من التهديدات المتزايدة التي قد تؤثر سلبا على الأداء والفعالية المؤسسية.
2. البيئة الرقمية هي بنية متكاملة من أدوات وتقنيات ومهارات رقمية وهي تعتمد على توافر إمكانيات تقنية مناسبة، وقدرات بشرية مؤهلة، وثقافة مؤسساتية رقمية حديثة.
3. العلاقة بين الأمن السيبراني والبيئة الرقمية علاقة تكاملية فكلما كانت ممارسات الأمن السيبراني متقدمة وفعالة، انعكس ذلك إيجابًا على استقرار البيئة الرقمية، مما يعزز من جودة الخدمات المقدمة ويزيد من ثقة المستخدمين.
4. الثقافة الرقمية والممارسات الواعية من طرف المستخدمين تمثل عنصراً داعماً للأمن السيبراني، حيث تساهم في تقليص الثغرات الناتجة عن السلوك البشري.
5. ضرورة دمج الأمن السيبراني في السياسات الرقمية للمؤسسات التعليمية، واعتباره مكونا استراتيجيا ضمن خطط تطوير التعليم الجامعي، خاصة في ظل التوجه نحو التعليم الإلكتروني والجامعات الذكية.

- ضعف الأمن السيبراني يعرّض البيئة الرقمية للاختراقات والمخاطر التي تؤثر على جودة الخدمات الرقمية ومصداقيتها.

II. النتائج التطبيقية:

أما على المستوى التطبيقي، ومن خلال تحليل البيانات المستخلصة من استبيان الأساتذة بجامعة محمد خيضر بسكرة، فقد تم التوصل إلى النتائج التالية:

- وجود وعي نسبي بأهمية الأمن السيبراني داخل الجامعة، يتجلى في الالتزام باستخدام البرمجيات المعتمدة، ووجود إجراءات للوقاية من المخاطر الرقمية.
- ضعف بعض الجوانب المرتبطة بالبنية التحتية الرقمية، خاصة ما يتعلق بعدم اقتناع الأساتذة بتخصيص ميزانيات دورية لتطويرها، مما يشير إلى الحاجة لمزيد من الاستثمار في الجانب التقني.
- اتجاه إيجابي عام نحو المهارات الرقمية، حيث أظهرت النتائج أن معظم أفراد العينة يسعون لتطوير قدراتهم بشكل ذاتي أو من خلال تكوينات، ما يعزز من جاهزيتهم للتفاعل مع متطلبات البيئة الرقمية.
- الثقافة الرقمية لدى الأساتذة متقدمة نسبيا، وتتميز باحترام الخصوصية، والتعامل الواعي مع المعطيات الرقمية، مما يدل على بيئة مهنية رقمية صحية.
- وجود تباين في تقييم الاستجابة المؤسسية لمشكلات الأمن الرقمي، حيث أظهرت بعض النتائج أن هناك شكوكا بشأن مدى جدية الإدارة في معالجة التهديدات الرقمية، مما يستدعي تدخلا استراتيجيا على مستوى الحوكمة الرقمية.
- البيئة الرقمية داخل الجامعة تتطور تدريجيا ولكنها بحاجة إلى دعم مؤسساتي مستدام، خصوصا في مجالات البنية التحتية، وتكوين الكوادر البشرية.

III. اختبار الفرضيات :

انطلاقا من الإطار النظري والدراسة الميدانية، سيتم في هذا الجزء تحليل الفرضيات المطروحة بهدف التحقق من مدى تحققها في ضوء النتائج المتوصل إليها. ويأتي هذا التحليل لتقييم فعالية دور الامن السيبراني في البيئة الرقمية.

- **الفرضية الرئيسية: "هناك دور ذو دلالة احصائية للأمن السيبراني في تحسين البيئة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)."**

أظهرت نتائج التحليل الإحصائي هناك دور ذو دلالة احصائية للأمن السيبراني في تحسين البيئة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05) وهذا ما يعني صحة الفرضية الرئيسية.

- **الفرضية الأولى الفرعية: هناك دور ذو دلالة احصائية للأمن السيبراني في تحسين البنية التحتية الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)."**

أظهرت نتائج التحليل الإحصائي ان هناك دور ذو دلالة احصائية للأمن السيبراني في تحسين البنية التحتية الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)." وهذا ما يعني صحة الفرضية الفرعية الأولى.

- **الفرضية الثانية الفرعية: " هناك دور ذو دلالة احصائية للأمن السيبراني في تحسين المهارات الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05).**

أظهرت نتائج التحليل الإحصائي ان هناك دور ذو دلالة احصائية للأمن السيبراني في تحسين المهارات الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05). وهذا ما يعني صحة الفرضية الفرعية الثانية.

- **الفرضية الثالثة الفرعية : هناك دور ذو دلالة احصائية للأمن السيبراني في تحسين الثقافة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)."**

أظهرت نتائج التحليل الإحصائي ان ليس هناك دور ذو دلالة احصائية للأمن السيبراني في تحسين الثقافة الرقمية بجامعة محمد خيضر بسكرة عند مستوى الدلالة (0.05)، وهذا ما يعني عدم صحة الفرضية الفرعية الثالثة.

IV. الاقتراحات:

في ضوء الإطار النظري للدراسة، والنتائج التي أسفرت عنها الإستبانة نقدم الاقتراحات التالية:

- وضع استراتيجية مؤسساتية واضحة للأمن السيبراني تشمل التكوين المستمر، وتحديث الأنظمة، والاستجابة للطوارئ.
- تعزيز التوعية الرقمية للطلبة والموظفين من خلال تنظيم دورات تكوينية منتظمة حول المخاطر السيبرانية وسبل الوقاية منها.
- رفع مستوى الاستثمار في البنية التحتية الرقمية، خاصة في مجال تخزين البيانات السحابية الآمنة وتحديث المعدات الرقمية.
- إدماج مبادئ الأمن السيبراني في المناهج الأكاديمية، خاصة في التخصصات التقنية والإدارية.
- تطوير آليات الرقابة والتقييم الدوري لسياسات الأمن الرقمي في الجامعة.

V. الآفاق والمقترحات البحثية:

أثارت انتباهنا ونحن نختتم هذا البحث عدة مواضيع أخرى للبحث في هذا المجال ونحبذ لو يعالجها باحثون آخرون في المستقبل وتتمثل بعض الإشكاليات المفتوحة فيما يلي:

- توسيع نطاق البحث ليشمل جامعات ومؤسسات تعليمية أخرى للمقارنة ومعرفة مدى تطبيق سياسات الأمن السيبراني على المستوى الوطني.
- دراسة تأثير التقدم في الذكاء الاصطناعي على تطوير نظم الأمن السيبراني في البيئة الجامعية.
- اقتراح نموذج تكاملي للأمن السيبراني يمكن تطبيقه في المؤسسات الجامعية الجزائرية مع مراعاة خصوصيات كل مؤسسة.
- البحث في الأبعاد الاجتماعية والنفسية المرتبطة باستخدام الأدوات الرقمية وتأثيرها على الفاعلية التعليمية داخل المؤسسات.
- إجراء دراسات كمية ونوعية أعمق حول مدى وعي الطلبة بمخاطر الاستخدام السيبراني، باعتبارهم من الفئات المستهدفة مباشرة في البيئة الرقمية.

فهرس المحتويات

فهرس المحتويات

قائمة المصادر والمراجع

قائمة المراجع

أولا: المراجع باللغة العربية:

I. الكتب:

1. اوس مجيد غالب العوادي. (2016). *الامن المعلوماتي السيبراني*. بغداد، العراق: مركز البيان للدراسات والتخطيط.
2. حسين وليد حسين عباس، و عبد الناصر حافظ علك. (2014). *نظم المعلومات الإدارية بالتركيز على وظائف المنظمة*. عمان، الاردن: دار غيداء للنشر و التوزيع.
3. حيدر شاكر النوري، و محمود حسن جمعة. (2015). *دراسات في أثر المعرفة وتكنولوجيا المعلومات في المنظمات*. جامعة ديالي، العراق: المطبعة المركزية .
4. عصام الدين مصطفى صالح. (2020). *اقتصاديات تكنولوجيا المعلومات والإعلان الإلكتروني في عصرالعولمة في المجتمعات العربية*. الاسكندرية، مصر: دار الفكر الجامعي.
5. علي زياد العلي. (2017). *المرتكزات النظرية في السياسة*. القاهرة، مصر: دار الفجر للنشر والتوزيع.
6. فارس محمد العمارات. (2022). *الامن السيبراني المفهوم وتحديات العصر*. عمان، الاردن: دار الخليج للنشر والتوزيع.
7. ليلى حسام الدين احمد شكر. (2011). *اثر التقدم في تكنولوجيا المعلومات على الخصائص النوعية و الكمية للموارد البشرية*. القاهرة، مصر: المنظمة العربية للتنمية الادارية جامعة الدول العربية.

II. المقالات و المؤتمرات:

1. ادريس عطية. (1 7, 2019). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. *مجلة المصداقية، 2*.
2. إسراء شريف جيجان. (2021). الأمن السيبراني الصيني: دراسة في الدوافع والتحديات. *قضايا سياسية، 65*.
3. بدر عدنان احمد سعد الخبيزي. (03 09, 2023). تحديات وتهديدات الامن السيبراني وكيفية التغلب عليه. *حوليات آداب عين شمس، 51*.
4. بن علية بن جدو. (2022). تحديات الأمن السيبيراني لمواجهة الجريمةالالكرتونية. *المجلة الجزائرية للامن الانساني، 07*.
5. حياة حميدي، و نسيمة طايلب. (01 11, 2022). مدخل مفاهيمي حول الألمن السيبراني. *مجلة مدار للدراسات الاتصالية الرقمية، 2*.
6. دعاء محمد محمود ابراهيم نجم. (2022). ماهية المجتمع الرقمي. *مجلة الخدمة الاجتماعية، 73*.
7. رحاب فايز احمد السيد، و عمر حوتيه. (30 03, 2023). المكتبات الجامعية الرقمية كانموذج للتحول نحو العمل في البيئة الرقمية. *مجلة ببليوفيليا للدراسات المكتبات والمعلومات*.
8. رشيد بن راشد، و حسينة بلحاح. (23 03, 2022). البيئة الرقمية: النظريات الإعلامية والميديا الجديدة. *مجلة المعيار، 12*.
9. سرى غضبان غيدان، و محمد منذر جلال الربيعي. (12, 2020). الامن السيبراني وسياسات المواجهة الدولية. *مجلة الدراسات الاستراتيجية والعسكرية*.

10. سمير بارة. (01 07, 2017). الأمن السيبراني (cyber Security) في الجزائر:السياسات و المؤسسات. *المجلة الجزائرية للامن الانساني، 2*.

11. عبد الجليل طواهير. (31 03, 2023). إستراتيجيات الأمن السيبراني كتحدي لتحول الرقمية بالمنظمات الحكومية مع الاشارة لتجربة دولة الإمارات العربية المتحدة. *مجلة الرسالة للدراسات الاعلامية، 7*.

12. عنترة بن مرزوق، و محي الدين حرشاوي. (06 06, 2017). الامن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية. *مجلة الباحث في العلوم الانسانية والاجتماعية*.

13. فاطمة الزهرة بليج، و صونيا قوراري . (21 06, 2024). دور البيئة الرقمية في تشكيل الثقافة المقاولاتية والمؤسسات الناشئة دراسة مسحية على عينة من متابعي صفحة دار المقاوللاتية لجامعة بسكرة على الفايسبوك. *مجلة الرسالة للدراسات والبحوث الانسانية*.

14. فطيمة لواعر. (15 07, 2023). الملكية الفكرية في البيئة الرقمية. *مجلة الحوكمة والقانون الاقتصادي، 03*.

15. فيروز يونس زازل. (14 03, 2024). واقع استجابت البيئة الرقمية في عملية التكوين التكميلي لفائدة طلبة سنة أولى دكتوراه بجامعة محمد بوضياف المسيلة. *مجلة المصباح في علم النفس وعلوم التربية والأرطوفونيا، 01*.

16. ليلى بن برغوث. (31 3, 2023). الامن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي التهديدات، التقنيات ، التحديات واليات التصدي. *المجلة الدولية للاتصال الاجتماعي، 01*.

17. محمد دحماني. (30 11, 2023). الذكاء الاصطناعي كألية لتعزيز الامن السيبراني. *مجلة الفكر القانوني وسياسي، 2*.

18. مني عبد الله السمحان. (2020). متطلبات تحقيق الامن السيبراني لانظمة المعلومات الادارية بجامعة الملك سعود. *مجلة كلية التربية*.

19. مولود بوخباش، و عيسى يحة. (30 10, 2019). تأثير البيئة الرقمية على مكونات الإستراتيجية التسويقية دراسة حالة موقع امازون. *مجلة الاصلاحات الاقتصادية والاندماج في الاقتصاد العالمي، 13*.

20. نجاة ساسي هادف. (10 6, 2022). إدارة وتسيير الموارد البشرية في البيئة الرقمية تحديات وآفاق. *مجلة علوم الانسان والمجتمع، 02*.

21. ياسر محمد هوساوي. (4 3, 2020). دور التوعية بالأمن السيبراني في الحد من أثر تعقيد وسائل التحقق الرقمي من الهوية على سلوك المستخدم الطرفي. *مجلة جامعة ام القرى للهندسة والعمارة، 11*.

III. الاطروحات والدكتوراه:

1. ايمان نوي. (2016). البيئة الرقمية وعلاقتها بالاغتراب الثقافي عند طلبة الجامعيين دراسة ميدانسة على عينة من طلبة جامعة محمد خيضر بسكرة المستخدمين لبعدي البيئة الرقمية. *اطروحة دكتوراه في علم الاجتماع*. بسكرة، الجزائر: جامعة محمد خيضر.

2. جمال بوازدية. (2021). الامن السيبراني. *محاضرات مقدمة لطلبة السنة الثانية ماستر*. الجزائر، الجزائر: جامعة الجزائر -03-.

3. عتيقة لحواطي. (2014). إسترجاع المعلومات العلمية والتقنية في ظل البيئة الرقمية ودوره في دعم الإتصال العلمي بين الباحثين دراسة ميدانية مع الأساتذة الباحثين بجامعة محمد الصديق بن يحيى- جيجل. *اطروحة دكتوراه عي علم اللمكتبات والتوثيق*.

قسنطينة، الجزائر: جامعة قسنطينة -02-محمد توفيق ومان. (2016). تنمية الموارد البشرية في ظل البيئة الرقمية دراسة في الابعاد السوسيو-تقنية حالة مديرية الأمن لولاية بسكرة. *اطروحة دكتوراه في علم الاجتماع*. بسكرة، الجزائر: جامعة محمد خيضر.

4. نسيمة ضيف الله. (2017/2016). استخدام تكنولوجيا المعلومات والاتصال وأثره على تحسين جودة العملية التعليمية: دراسة عينة من الجامعات الجزائرية. *اطروحة دكتوراه في علوم التسيير*. باتنة، الجزار: جامعة الحاج لخضر.
5. ياسمينة ياسع. (2011). دراسة اقتصادية قياسية لاثر تكنولوجيا المعلومات و الاتصالات على الاداءالاقتصادي للمنظمة دراسة حالة شركة القطن الممتص. *مذكرة ماجستير في العلوم الاقتصادية*. بومرداس، الجزائر: جامعة امحمد بوقرة

ثانيا:المراجع بالغة الاجنبية

1. *Cyber security threats*. (2024). تم الاسترداد من data Guard: https://www.dataguard.com/cyber-/security/threats
2. Humayun Bakht. (2020). *الامن السيبراني*.
3. maryville university. (2024, 06 24). *The History of Cybersecurity*. Retrieved from maryville university: https://online.maryville.edu/blog/history-of-cybersecurity/

.

الملاحق

الملحق (01): استبانة الدراسة

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم والبحث العلمي

جامعة محمد خيضر بسكرة

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

تخصص اقتصاد رقمي

استبيان حول

دور الأمن السيبراني في تحسين البيئة الرقمية

دراسة حالة جامعة محمد خيضر بسكرة ".

الى السيد (ة):

في اطار تحضير رسالة ماستر02 تحت عنوان " **دور الأمن السيبراني في تحسين البيئة الرقمية دراسة حالة جامعة محمد خيضر بسكرة** " نرجو من سيادتكم المحترمة الاجابة على الاستبانة التالية وذلك من اجل مساعدتنا في جمع المعلومات اللازمة حول الموضوع. كما نحيطكم علما ان جميع الاجابات والمعلومات التي تدلون ستبقى سرية ولا يتم استخدامها الا في غرض البحث العلمي.

وفي الاخير تقبلوا منا أسمى عبارات الشكر والتقدير

الطالبة:

- **أميرة ندى الريحان سماتي.**

الأستاذ المشرف:

- **بن الزاوي عبد الرزاق.**

السنة الجامعية: 2025/2024

✓ القسم الاول: لبيانات الشخصية

يرجى منكم وضع علامة (✓) في المربع المناسب لاختيارك

1- الجنس: ذكر ☐ أنثى ☐

2- العمر: أقل من 30 سنة ☐ من 30 إلى أقل من 40 سنة ☐

من 40 إلى أقل من 50 سنة ☐ من 50 سنة فأكثر ☐

3- الخبرة: **اقل من 5 سنوات** ☐ من 5 سنوات الى اقل من 10 سنوات ☐

من 10 سنوات الى اقل من 15 سنوات ☐ أكثر من 15 سنة ☐

4- الرتبة: أستاذ مساعد –أ– ☐ من أستاذ مساعد–ب– ☐

أستاذ محاضر–أ– ☐ أستاذ محاضر–ب– . ☐

أستاذ تعليم عالي ☐

5- الكلية : كلية العلوم الاقتصادية و التجارية و علوم التسيير ☐

كلية الآداب و اللغات ☐

كلية الهندسة المعمارية ☐

كلية العلوم و التكنولوجيا ☐

✓ **القسم الثاني.**

المحور الأول: الأمن السيبراني يعد الأمن السيبراني من المتطلبات الجوهرية لضمان سلامة المعلومات والبنية التقنية في المؤسسات التعليمية، خصوصًا مع تزايد الاعتماد على الأنظمة الرقمية في التدريس والإدارة، ويسعى هذا الجزء من الاستبيان إلى قياس وعي أعضاء هيئة التدريس بمستوى الأمن السيبراني المطبق في جامعتهم، والسياسات المتبعة لحماية البيانات الأكاديمية من التهديدات الرقمية

الرقم	الفقرة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
01	توجد سياسة واضحة للأمن السيبراني في المؤسسة الجامعية.					
02	تنظيم تدريبات للموظفين على أساسيات الأمن السيبراني بشكل منتظم.					
03	استخدام برامج وتطبيقات موثوقة للحماية من الاختراقات والبرمجيات الخبيثة					
04	يُسمح فقط باستخدام البرمجيات المعتمدة على الأجهزة الجامعية.					
05	ايجاد اليات للإبلاغ عن التهديدات الأمنية الرقمية اتصال خارجية.					
06	يتم اتخاذ إجراءات فعلية بعد الإبلاغ عن التهديدات أو الحوادث الأمنية					
07	تعتقد أن الطلاب والموظفين بحاجة إلى برامج توعوية مستمرة حول الأمن السيبراني					
08	يتم تحديث الأنظمة التشغيلية والتطبيقات بانتظام داخل الجامعة					
09	تعتقد أن الشبكة الداخلية للجامعة آمنة بما فيه الكفاية					
10	تترك أجهزتك مفتوحة أو غير مؤمّنة عند الابتعاد عنها					
11	تقوم بفحص الروابط أو المرفقات قبل فتحها عبر البريد الإلكتروني					
12	تستخدم كلمات مرور قوية ومختلفة لحساباتك الجامعية.					

المحور الثاني: البيئة الرقمية

البنية التحتية الرقمية تُشكّل الأساس الذي تُبنى عليه البيئة التعليمية الرقمية، وتشمل التجهيزات التقنية، الاتصال بالشبكة، وتوافر البرامج والأنظمة يهدف هذا الجزء إلى تقييم مدى كفاءة وفاعلية البنية التحتية المتاحة لعضو هيئة التدريس، وأثرها في تمكين العملية التعليمية الرقميةو لا يكفي وجود البنية التحتية فقط، بل يتطلب نجاح البيئة الرقمية امتلاك الكادر الأكاديمي للمهارات والثقافة اللازمة لاستخدام الأدوات والتقنيات الحديثة بفعالية

الملاحق

الرقم	الفقرة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
	اولا: البنية التحتية الرقمية					
01	توافر شبكة انترنت مستقرة وسريعة في بيئة العمل					
02	اجراء تحديثات للأجهزة الرقمية والبرمجيات المستخدمة بشكل دوري					
03	توفير خوادم امنة ومساحات تخزين سحابية موثوقة لحفظ البيانات					
04	صيانة البنية التحتية الرقمية بانتظام لضمان الاستمرارية					
05	تخصيص ميزانيات دورية لتطوير البنية التحتية التقنية					
06	يتم فحص أمان الخوادم بشكل منتظم لحماية المعلومات من الاختراقات					
	ثانيا: المهارات الرقمية					
07	أمتلك القدرة على استخدام البرمجيات الأساسية في بيئة العمل					
08	أستطيع التعامل مع الأنظمة الرقمية المستخدمة بكفاءة والمنصات التعليمية					
09	أتمكن من حماية بياناتي الشخصية والمهنية الكترونيا					
10	تمكن من التعلم الذاتي عبر الأنترنت لتعزيز مهاراتي الرقمية					
11	أطور مهاراتي الرقمية من خلال التدريب الذاتي أو الرسمي					
	ثالثا: الثقافة الرقمية					
12	تدرك أهمية السلوك الرقمي المسؤول عند استخدام الأنترنت					
13	تلتزم بالقوانين والأنظمة المتعلقة بالاستخدام الرقمة					
14	ادارة الجامعة تتعامل بجدية مع مشكلات الأمن الرقمي					
15	تحرص على احترام خصوصية الاخرين في البيئات الرقمية					
16	تشعر بالثقة عند استخدام البريد الالكتروني الجامعي					

شاكرين لكم حسن تعاونكم

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	36	100.0
	Excluded[a]	0	.0
	Total	36	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.847	12

```
RELIABILITY
  /VARIABLES=y1.1 y1.2 y1.3 y1.4 y1.5 y1.6
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA.
```

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	36	100.0
	Excluded[a]	0	.0
	Total	36	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.803	6

```
RELIABILITY
  /VARIABLES=y2.1 y2.2 y2.3 y2.4 y2.5
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA.
```

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	36	100.0
	Excluded[a]	0	.0
	Total	36	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.702	5

```
RELIABILITY
  /VARIABLES=y3.1 y3.2 y3.3 y3.4 y3.5
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA.
```

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	36	100.0
	Excluded[a]	0	.0
	Total	36	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.266	5

```
RELIABILITY
  /VARIABLES=Y1 Y2 Y3
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA.
```

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	36	100.0
	Excluded[a]	0	.0
	Total	36	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.688	3

```
RELIABILITY
  /VARIABLES=X Y
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA.
```

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	36	100.0
	Excluded[a]	0	.0
	Total	36	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.906	2

```
CORRELATIONS
  /VARIABLES=X x1 x2 x3 x4 x6 x5 x7 x8 x9 x10 x11 x12
  /PRINT=TWOTAIL NOSIG
  /MISSING=PAIRWISE.
```

Correlations

Correlations

		X	x1	x2	x3	x4	x6
X	Pearson Correlation	1	.417*	.606**	.750**	.540**	.745**
	Sig. (2-tailed)		.011	.000	.000	.001	.000
	N	36	36	36	36	36	36
x1	Pearson Correlation	.417*	1	.412*	.491**	.095	.399*
	Sig. (2-tailed)	.011		.013	.002	.581	.016
	N	36	36	36	36	36	36
x2	Pearson Correlation	.606**	.412*	1	.458**	.682**	.436**
	Sig. (2-tailed)	.000	.013		.005	.000	.008
	N	36	36	36	36	36	36
x3	Pearson Correlation	.750**	.491**	.458**	1	.324	.640**
	Sig. (2-tailed)	.000	.002	.005		.054	.000
	N	36	36	36	36	36	36
x4	Pearson Correlation	.540**	.095	.682**	.324	1	.302
	Sig. (2-tailed)	.001	.581	.000	.054		.074
	N	36	36	36	36	36	36
x6	Pearson Correlation	.745**	.399*	.436**	.640**	.302	1
	Sig. (2-tailed)	.000	.016	.008	.000	.074	
	N	36	36	36	36	36	36
x5	Pearson Correlation	.677**	.096	.212	.465**	.111	.304
	Sig. (2-tailed)	.000	.579	.215	.004	.518	.071
	N	36	36	36	36	36	36
x7	Pearson Correlation	.725**	.214	.264	.635**	.169	.466**
	Sig. (2-tailed)	.000	.210	.120	.000	.326	.004
	N	36	36	36	36	36	36
x8	Pearson Correlation	.651**	-.016	.267	.531**	.508**	.365*
	Sig. (2-tailed)	.000	.925	.116	.001	.002	.029
	N	36	36	36	36	36	36
x9	Pearson Correlation	.772**	.275	.375*	.450**	.318	.690**
	Sig. (2-tailed)	.000	.104	.024	.006	.059	.000
	N	36	36	36	36	36	36
x10	Pearson Correlation	.584**	.213	.233	.237	.142	.327
	Sig. (2-tailed)	.000	.213	.171	.163	.409	.051
	N	36	36	36	36	36	36
x11	Pearson Correlation	.633**	.156	.378*	.336*	.336*	.480**
	Sig. (2-tailed)	.000	.364	.023	.045	.045	.003
	N	36	36	36	36	36	36

x12	Pearson Correlation	.111	-.121	-.141	-.213	.080	-.053
	Sig. (2-tailed)	.519	.481	.410	.213	.643	.759
	N	36	36	36	36	36	36

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

```
CORRELATIONS
  /VARIABLES=Y Y1 Y2 Y3
  /PRINT=TWOTAIL NOSIG
  /MISSING=PAIRWISE.
```

Correlations

Correlations

		Y	Y1	Y2	Y3
Y	Pearson Correlation	1	.906**	.900**	.479**
	Sig. (2-tailed)		.000	.000	.003
	N	36	36	36	36
Y1	Pearson Correlation	.906**	1	.748**	.190
	Sig. (2-tailed)	.000		.000	.267
	N	36	36	36	36
Y2	Pearson Correlation	.900**	.748**	1	.254
	Sig. (2-tailed)	.000	.000		.135
	N	36	36	36	36
Y3	Pearson Correlation	.479**	.190	.254	1
	Sig. (2-tailed)	.003	.267	.135	
	N	36	36	36	36

**. Correlation is significant at the 0.01 level (2-tailed).

```
DESCRIPTIVES VARIABLES=X Y1 Y2 Y3 Y
  /STATISTICS=KURTOSIS SKEWNESS.
```

Descriptives

Descriptive Statistics

	N	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Std. Error
X	36	-.919	.393	1.643	.768
Y1	36	-1.272	.393	1.758	.768
Y2	36	-1.130	.393	1.868	.768
Y3	36	-.154	.393	.143	.768
Y	36	-1.343	.393	2.628	.768
Valid N (listwise)	36				

```
FREQUENCIES VARIABLES=الجنس السن الخبرة الرتبة الكلية
  /ORDER=ANALYSIS.
```

Frequencies

Statistics

		الجنس	السن	الخبرة	الرتبة	الكلية
N	Valid	36	36	36	36	36
	Missing	0	0	0	0	0

Frequency Table

الجنس

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ذكر	15	41.7	41.7	41.7
	انثى	21	58.3	58.3	100.0
	Total	36	100.0	100.0	

السن

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	اقل من 30 سنة	5	13.9	13.9	13.9
	من 30 الى 40	17	47.2	47.2	61.1
	من 41 الى 50 سنة	11	30.6	30.6	91.7
	سنة فاكر 51	3	8.3	8.3	100.0
	Total	36	100.0	100.0	

الخبرة

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	اقل من 5 سنوات	7	19.4	19.4	19.4
	من 5الى 10سنوات	16	44.4	44.4	63.9
	من 11 الى 15 سنة	8	22.2	22.2	86.1
	من 15 سنة فاكر	5	13.9	13.9	100.0
	Total	36	100.0	100.0	

الرتبة

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	استاذ مساعد ب	6	16.7	16.7	16.7
	استاذ مساعد ا	5	13.9	13.9	30.6
	استاذ محاضر ب	14	38.9	38.9	69.4
	استاذ محاضر ا	9	25.0	25.0	94.4
	استاذ دكتور	2	5.6	5.6	100.0
	Total	36	100.0	100.0	

الكلية

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	كلية العلوم الاقتصادية و التجارية و علوم التسيير	19	52.8	52.8	52.8
	كلية الادب و الغات	14	38.9	38.9	91.7
	كلية العلوم الدقيقة	1	2.8	2.8	94.4

	كلية العلوم و التكنولوجيا	2	5.6	5.6	100.0
	Total	36	100.0	100.0	

```
DESCRIPTIVES VARIABLES=x1 x2 x3 x4 x6 x5 x7 x8 x9 x10 x11 x12 X y1.1 y1.2
y1.3 y1.4 y1.5 y1.6 Y1
    y2.1 y2.2 y2.3 y2.4 y2.5 Y2 y3.1 y3.2 y3.3 y3.4 y3.5 Y3 Y
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Descriptives

Descriptive Statistics

	N	Mean	Std. Deviation
x1	36	3.64	.762
x2	36	3.69	.822
x3	36	3.44	1.206
x4	36	3.89	1.008
x6	36	3.44	1.107
x5	36	3.25	1.273
x7	36	3.53	1.028
x8	36	3.58	.967
x9	36	3.50	1.159
x10	36	3.42	1.131
x11	36	3.44	.909
x12	36	3.86	.867
X	36	3.5579	.62925
y1.1	36	3.06	1.218
y1.2	36	3.42	1.052
y1.3	36	3.69	.980
y1.4	36	3.28	1.256
y1.5	36	2.97	.971
y1.6	36	3.33	1.121
Y1	36	3.2917	.78414
y2.1	36	3.56	.877
y2.2	36	3.81	.980
y2.3	36	3.33	1.069
y2.4	36	3.03	1.134
y2.5	36	3.83	.697
Y2	36	3.5111	.65106

y3.1	36	3.61	.766
y3.2	36	4.00	.793
y3.3	36	3.25	1.052
y3.4	36	4.06	.630
y3.5	36	4.00	.632
Y3	36	3.7833	.39821
Y	36	3.5287	.49571
Valid N (listwise)	36		

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT X
  /METHOD=ENTER Y1.
```

Regression

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Y1[b]	.	Enter

a. Dependent Variable: X

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.883[a]	.780	.774	.29938

a. Predictors: (Constant), Y1

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.811	1	10.811	120.627	.000[b]
	Residual	3.047	34	.090		

	Total	13.859	35			

a. Dependent Variable: X

b. Predictors: (Constant), Y1

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.225	.218		5.613	.000
	Y1	.709	.065	.883	10.983	.000

a. Dependent Variable: X

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT X
  /METHOD=ENTER Y2.
```

Regression

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Y2[b]	.	Enter

a. Dependent Variable: X

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.742[a]	.550	.537	.42822

a. Predictors: (Constant), Y2

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.624	1	7.624	41.578	.000[b]
	Residual	6.235	34	.183		
	Total	13.859	35			

a. Dependent Variable: X

b. Predictors: (Constant), Y2

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.041	.397		2.623	.013
	Y2	.717	.111	.742	6.448	.000

a. Dependent Variable: X

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT X
  /METHOD=ENTER Y3.
```

Regression

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Y3[b]	.	Enter

a. Dependent Variable: X

b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.226[a]	.051	.023	.62188

a. Predictors: (Constant), Y3

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.710	1	.710	1.835	.184[b]
	Residual	13.149	34	.387		
	Total	13.859	35			

a. Dependent Variable: X

b. Predictors: (Constant), Y3

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.205	1.004		2.196	.035
	Y3	.358	.264	.226	1.355	.184

a. Dependent Variable: X

```
REGRESSION
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT X
  /METHOD=ENTER Y.
```

Regression

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Y[b]	.	Enter

a. Dependent Variable: X

b. All requested variables entered.

الملاحق

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.851[a]	.724	.716	.33524

a. Predictors: (Constant), Y

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.037	1	10.037	89.310	.000[b]
	Residual	3.821	34	.112		
	Total	13.859	35			

a. Dependent Variable: X

b. Predictors: (Constant), Y

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	-.254	.407		-.624	.537
	Y	1.080	.114	.851	9.450	.000

a. Dependent Variable: X