

أثر الأمن السيبراني على نجاح و كفاءة إدارة المشاريع الرقمية :دراسة تطبيقية

وفاء ماجد حسين البرقوني

مشروع تخرج – ٢
كلية الإدارة -جامعة ميدأوشن

إشراف

د. عبدالرحيم نادر

عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

2026

الشكر والتقدير

الحمد لله أولاً وآخرًا، الذي بنعمته تتم الصالحات، والصلاة والسلام على سيدنا محمد صلى الله عليه وسلم.

أتقدم بخالص الشكر والتقدير إلى جامعة ميدأوشن ممثلة بكلية الإدارة، لما وفرتة من بيئة تعليمية ساهمت في تنمية معارفنا وصقل مهارتنا خلال فترة الدراسة.

كما أتقدم بجزيل الشكر والتقدير إلى مشرف المشروع الدكتور/ عبدالرحيم نادر على توجيهاته القيمة، وملاحظاته البناءة، ودعمه المستمر الذي كان له الأثر الكبير في إنجاز هذا المشروع.

ولا يفوتني أن أتقدم بالشكر لكل من ساهم في تعبئة الاستبيان، ولكل من قدم لي المساعدة أو الدعم أو النصيحة خلال إعداد هذا البحث.

وفي الختام، أسأل الله تعالى أن يجعل هذا العمل خالصًا لوجهه الكريم، وأن ينفع به، وأن يوفقنا جميعًا لما يحب ويرضى.

الإهداء

إلى من كان دعاؤهم سرّ نجاحي، وإلى من غمروني بالمحبة والدعم في جميع مراحل حياتي
إلى والديّ العزيزين، حفظهما الله وأدام عليهما الصحة والعافية، عرفاناً بفضلهما وصبرهما وتشجيعهما المستمر
وإلى أسرتي الكريمة، وكل من وقف إلى جانبي وساندني بالكلمة الطيبة والدعاء الصادق
وإلى أساتذتي الأفاضل، الذين أناروا لنا طريق العلم والمعرفة
أهدي هذا العمل المتواضع، راجياً من الله أن يكون ثمرةً نافعة، وأن يكلل جهود الجميع بالتوفيق والنجاح

مستخلص الدراسة

الهدف:

هدفت هذه الدراسة إلى التعرف على أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية، وبيان دوره في تقليل المخاطر والحد من احتمالية تأخير أو فشل المشاريع، بالإضافة إلى دراسة العلاقة بين مستوى تطبيق ممارسات الأمن السيبراني ونجاح المشاريع الرقمية.

المنهجية:

اعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت الاستبيان كأداة رئيسية لجمع البيانات من عينة من العاملين في مجال إدارة المشاريع الرقمية وتقنية المعلومات. وتم تحليل البيانات باستخدام البرنامج الإحصائي (SPSS)، بالاعتماد على الأساليب الإحصائية المناسبة مثل المتوسطات الحسابية والانحرافات المعيارية واختبارات الارتباط والانحدار.

النتائج:

من المتوقع أن تسهم ممارسات الأمن السيبراني في تعزيز نجاح المشاريع الرقمية، وتحسين كفاءة إدارتها، وتقليل المخاطر المرتبطة بها، كما تشير الدراسة إلى وجود علاقة إيجابية بين تطبيق ممارسات الأمن السيبراني وتحقيق أهداف المشاريع الرقمية.

التطبيقات والأهمية:

تسهم نتائج الدراسة في توعية المؤسسات ومديري المشاريع بأهمية دمج ممارسات الأمن السيبراني في جميع مراحل إدارة المشاريع الرقمية، بما يحقق استمرارية الأعمال، ويحسن جودة الأداء، ويحد من المخاطر والتهديدات الإلكترونية.

الكلمات المفتاحية:

الأمن السيبراني، إدارة المشاريع الرقمية، نجاح المشاريع، كفاءة إدارة المشاريع، تقليل المخاطر.

جدول المحتويات

الشكر والتقدير.....	خطأ! الإشارة المرجعية غير معرفة.
الإهداء.....	خطأ! الإشارة المرجعية غير معرفة.
مستخلص الدراسة.....	خطأ! الإشارة المرجعية غير معرفة.
١. الفصل الأول: الإطار العام للدراسة.....	خطأ! الإشارة المرجعية غير معرفة.
١,١. المقدمة:	خطأ! الإشارة المرجعية غير معرفة.
١,٢. مشكلة الدراسة.....	خطأ! الإشارة المرجعية غير معرفة.
١,٢,١. فجوات على المستوى النظري.....	خطأ! الإشارة المرجعية غير معرفة.
١,٢,٢. فجوات على المستوى التطبيقي.....	خطأ! الإشارة المرجعية غير معرفة.
١,٣. أهمية الدراسة.....	١٠
١,٣,١. على المستوى النظري:	١٠
١,٣,٢. على المستوى التطبيقي:	١٠
١,٤. أسئلة الدراسة.....	خطأ! الإشارة المرجعية غير معرفة.
١,٥. أهداف الدراسة.....	١١
١,٦. فرضيات الدراسة.....	١١
١,٧. نموذج الدراسة.....	١١
١,٨. الدراسة الميدانية.....	١٤
١,٩. مخطط المشروع.....	١٧
٢. الفصل الثاني: الدراسات السابقة.....	١٩
٢,١. المقدمة:	٢٠
٢,٢. المتغير المستقل.....	٢١
٢,٣. المتغير التابع.....	٢٢
٢,٤. العلاقة بين المتغير المستقل والمتغير التابع.....	٢٣
٢,٥. الخاتمة.....	٢٧
٣. الفصل الثالث: منهجية الدراسة.....	٢٨
٣,١. المقدمة.....	٢٩
٣,٢. التعريفات الإجرائية لمتغيرات البحث.....	٢٩
٣,٣. تصميم البحث.....	٣٠
٣,٤. مجتمع البحث وطرق وتقنيات أخذ العينات.....	٣٠
٣,٥. طريقة جمع البيانات.....	٣١
٣,٦. أنواع البيانات.....	٣١

٣٢	٣,٧. إجراءات التحليل الإحصائي
٣٣	٣,٨. الخاتمة.....
٣٥	٤. الفصل الرابع: التحليل الإحصائي ومناقشة النتائج
٣٦	4.1. المقدمة.....
٣٦	4.2. توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث).....
٣٦	4.3. اختبارات الصدق والثبات للاستبيانات.....
٣٧	4.4. الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث)
٣٧	4.5. اختبار الفرضيات ومناقشة النتائج.....
٣٨	٤,٦. الخاتمة.....
٣٩	٥. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات.....
٤٠	٥,١. حدود الدراسة والدراسات المستقبلية:.....
٤٠	٥,٢. توصيات الدراسة:.....
٤١	٥,٣. الخاتمة:.....
٤٢	قائمة المراجع.....

1. الفصل الأول: الإطار العام للدراسة

1.1. المقدمة:

في ظل التطور الرقمي المتسارع الذي يشهده العالم، أصبحت إدارة المشاريع من الركائز الأساسية التي تعتمد عليها المؤسسات لتحقيق أهدافها بكفاءة وفعالية، خاصة في ظل التنافس المتزايد والتغيرات المستمرة في بيئة الأعمال. وقد ساهم التقدم التكنولوجي في تحويل العديد من المشاريع إلى بيئات رقمية تعتمد بشكل كبير على الأنظمة الإلكترونية والتطبيقات الحديثة.

ومع هذا التحول الرقمي، ظهرت تحديات جديدة تواجه إدارة المشاريع، من أبرزها المخاطر المرتبطة بالأمن السيبراني، والتي تشمل الهجمات الإلكترونية واختراق الأنظمة وتسريب البيانات. إذ يمكن أن تؤدي هذه التهديدات إلى تعطيل سير العمل، وزيادة التكاليف، والتأثير سلبًا على جودة مخرجات المشروع، مما ينعكس بشكل مباشر على نجاحه.

ويكتسب موضوع الأمن السيبراني أهمية متزايدة في ظل الاعتماد الكبير على التكنولوجيا، حيث أصبح عنصرًا أساسيًا في حماية معلومات المشاريع وضمان استمراريته. كما أن دمج ممارسات الأمن السيبراني ضمن عمليات إدارة المشاريع يساهم في تقليل المخاطر وتعزيز كفاءة الأداء وتحقيق الأهداف المرجوة.

ومن هذا المنطلق، تهدف هذه الدراسة إلى التعرف على أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية، من خلال تحليل دوره في تقليل المخاطر وتحسين جودة الأداء، بما يساهم في دعم استمرارية المشاريع وتحقيق نتائج أكثر فاعلية.

1.2. مشكلة الدراسة

في ظل التوسع الكبير في استخدام الأنظمة الرقمية في إدارة المشاريع، أصبحت المؤسسات تعتمد بشكل متزايد على التكنولوجيا في تخطيط وتنفيذ ومتابعة أعمالها. وعلى الرغم من هذا التطور، إلا أن العديد من المشاريع لا تزال تواجه تحديات تتعلق بحماية البيانات والأنظمة من التهديدات السيبرانية، مما قد يؤثر سلباً على كفاءة المشروع ونجاحه.

1.2.1. فجوات على المستوى النظري

تتمثل الفجوة على المستوى النظري في محدودية الدراسات التي تربط بشكل مباشر بين الأمن السيبراني وإدارة المشاريع، حيث يتم تناول كل منهما بشكل منفصل دون التركيز الكافي على العلاقة التكاملية بينهما.

1.2.2. فجوات على المستوى التطبيقي

أما على المستوى التطبيقي، فتظهر الفجوة في ضعف تطبيق ممارسات الأمن السيبراني داخل المشاريع الرقمية، حيث تركز بعض المؤسسات على الجوانب التقليدية لإدارة المشاريع مثل الوقت والتكلفة، مع إهمال الجوانب الأمنية، مما يزيد من احتمالية التعرض للمخاطر والاختراقات و ما يترتب عليهم من آثار سلبية قد تصل إلى تعثر المشروع أو فشله.

و انطلاقاً من ذلك، تتمثل مشكلة الدراسة في الإجابة عن السؤال الرئيسي التالي : " ما مدى تأثير الأمن

السيبراني على نجاح و كفاءة إدارة المشاريع الرقمية؟ "

1.3. أهمية الدراسة

1.3.1. على المستوى النظري:

تتبع أهمية هذه الدراسة من مساهمتها في إثراء الأدبيات العلمية المتعلقة بإدارة المشاريع والأمن السيبراني، من خلال توضيح العلاقة بينهما وبيان دور الأمن السيبراني كعامل مؤثر في نجاح المشاريع الرقمية. كما تسعى الدراسة إلى سد الفجوة المعرفية من خلال تقديم إطار نظري يربط بين مفاهيم إدارة المشاريع وممارسات الأمن السيبراني.

1.3.2. على المستوى التطبيقي:

تتمثل الأهمية التطبيقية لهذه الدراسة في تقديم نتائج وتوصيات عملية تساعد مديري المشاريع والمؤسسات على تعزيز ممارسات الأمن السيبراني ضمن مشاريعهم، بما يساهم في تقليل المخاطر وحماية البيانات وتحسين كفاءة الأداء. كما تساعد الدراسة في توجيه صناع القرار إلى أهمية دمج الجوانب الأمنية في مختلف مراحل إدارة المشروع لضمان نجاحه واستمراره.

1.4. أسئلة الدراسة

- ☐ ما أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية؟
- ☐ ما مستوى تطبيق ممارسات الأمن السيبراني في المشاريع الرقمية؟
- ☐ ما دور الأمن السيبراني في تقليل المخاطر التي تواجه المشاريع الرقمية؟
- ☐ هل يؤدي ضعف الأمن السيبراني إلى تأخير أو فشل المشاريع الرقمية؟
- ☐ ما العلاقة بين مستوى الحماية السيبرانية و تقليل المخاطر في المشاريع الرقمية؟

1.5. أهداف الدراسة

1. التعرف على أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية. 2. تحديد مستوى تطبيق ممارسات الأمن السيبراني في المشاريع الرقمية.
3. توضيح دور الأمن السيبراني في تقليل المخاطر التي تواجه المشاريع الرقمية. 4. تحليل تأثير ضعف الأمن السيبراني على تأخير أو فشل المشاريع الرقمية.
5. بيان العلاقة بين مستوى تطبيق الأمن السيبراني ونجاح المشاريع الرقمية.

1.6. فرضيات الدراسة

المتغير المستقل (الأمن السيبراني)

المتغيرات التابعة (نجاح المشاريع الرقمية – كفاءة إدارة المشاريع – تقليل المخاطر – فشل \ تأخير المشاريع)
(الفرضيات)

1. توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق ممارسات الأمن السيبراني ونجاح المشاريع الرقمية.
2. توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق الأمن السيبراني وكفاءة إدارة المشاريع الرقمية.
3. توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق الأمن السيبراني وتقليل المخاطر في المشاريع الرقمية.
4. توجد علاقة ذات دلالة إحصائية بين ضعف الأمن السيبراني وزيادة احتمالية تأخير أو فشل المشاريع الرقمية.

1.7. نموذج الدراسة

يعتمد هذا البحث على نموذج مفاهيمي يوضح العلاقة بين *الأمن السيبراني* كمتغير مستقل، و*نجاح وكفاءة إدارة المشاريع الرقمية* كمتغيرات تابعة، بالإضافة إلى دوره في *تقليل المخاطر* وتأثيره على *تأخير أو فشل المشاريع*.

ويفترض النموذج أن مستوى تطبيق ممارسات الأمن السيبراني يؤثر بشكل مباشر على نجاح المشاريع الرقمية وكفاءة إدارتها، كما يساهم في تقليل المخاطر التي قد تواجه هذه المشاريع. وفي المقابل، فإن ضعف الأمن السيبراني قد يؤدي إلى زيادة احتمالية تأخير المشاريع أو فشلها.

ويستخدم هذا النموذج لتوجيه منهجية البحث وتحليل البيانات، من خلال اختبار العلاقات بين المتغير المستقل والمتغيرات التابعة باستخدام الأساليب الإحصائية المناسبة.

يتكون نموذج البحث من العناصر التالية:

***المتغير المستقل:**

مستوى تطبيق ممارسات الأمن السيبراني

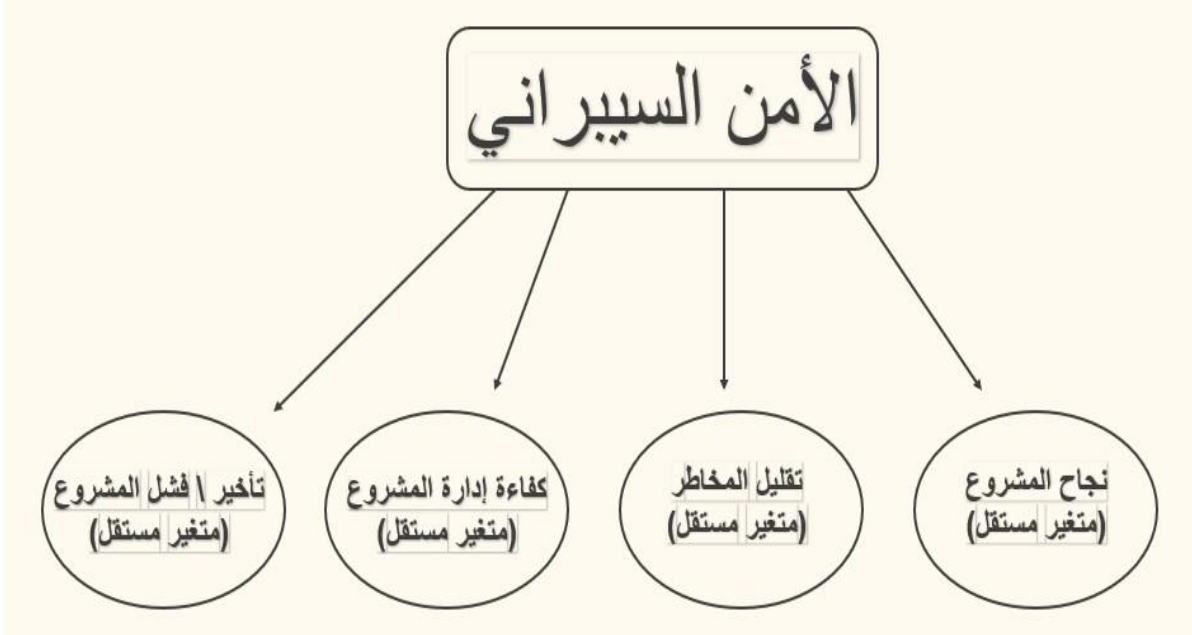
***المتغيرات التابعة:**

* نجاح المشاريع الرقمية

* كفاءة إدارة المشاريع الرقمية * تقليل

المخاطر

* تأخير أو فشل المشاريع



1.8. منهجية الدراسة

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، والذي يُعد من أكثر المناهج ملائمةً لدراسة الظواهر الإدارية وتحليل العلاقات بين المتغيرات، حيث يهدف إلى وصف واقع تطبيق ممارسات الأمن السيبراني في المشاريع الرقمية، وتحليل أثرها على نجاح وكفاءة إدارة المشاريع.

تصميم البحث

يعتمد البحث على التصميم الكمي (Quantitative Research Design)، وذلك من خلال جمع بيانات رقمية قابلة للتحليل الإحصائي، بهدف اختبار فرضيات الدراسة وقياس العلاقة بين المتغير المستقل (الأمن السيبراني) والمتغيرات التابعة (نجاح المشاريع، كفاءة الإدارة، تقليل المخاطر، وتأخير أو فشل المشاريع).

مجتمع الدراسة

يتكون مجتمع الدراسة من العاملين في مجال إدارة المشاريع الرقمية وتقنية المعلومات، بما في ذلك:

- * مدراء المشاريع
- * أعضاء فرق العمل في المشاريع الرقمية
- * المختصين في الأمن السيبراني داخل المؤسسات

عينة الدراسة

تم اختيار عينة الدراسة باستخدام أسلوب العينة العشوائية البسيطة، لضمان تمثيل عادل لمجتمع الدراسة، حيث سيتم توزيع الاستبيان على عدد من الأفراد العاملين في المجال.

ويمكن أن يتراوح حجم العينة بين (50 – 150) مشارك، بما يتناسب مع طبيعة الدراسة وإمكانية الوصول إلى المبحوثين.

أدوات جمع البيانات

تعتمد الدراسة على الاستبيان (Questionnaire) كأداة رئيسية لجمع البيانات، حيث تم تصميمه بناءً على محاور الدراسة، ويتكون من عدة أقسام، منها:

1. البيانات الديموغرافية (مثل: العمر، الخبرة، المسمى الوظيفي) 2. مستوى تطبيق ممارسات الأمن السيبراني
 3. مستوى نجاح المشاريع الرقمية 4. كفاءة إدارة المشاريع
 5. تقليل المخاطر
 6. تأثير ضعف الأمن السيبراني على تأخير أو فشل المشاريع
- ويتم قياس الإجابات باستخدام مقياس ليكرت الخماسي (من موافق بشدة إلى غير موافق بشدة).

تقنيات تحليل البيانات

سيتم تحليل البيانات باستخدام الأساليب الإحصائية المناسبة، ومن أبرزها:

الإحصاء الوصفي: مثل المتوسطات الحسابية والانحراف المعياري، لوصف خصائص العينة اختبار الارتباط (Correlation):

لقياس العلاقة بين المتغيرات

تحليل الانحدار (Regression Analysis): لاختبار تأثير الأمن السيبراني على المتغيرات التابعة

استخدام برامج إحصائية مثل SPSS لتحليل البيانات واستخراج النتائج

الاعتبارات الأخلاقية

تلتزم الدراسة بعدد من المبادئ الأخلاقية، من أهمها:

- * ضمان سرية معلومات المشاركين وعدم استخدامها إلا لأغراض البحث العلمي * استخدام البيانات بشكل جماعي دون الإشارة إلى أي أسماء أو معلومات شخصية * الحصول على موافقة المشاركين قبل تعبئة الاستبيان
- * توضيح هدف الدراسة للمشاركين بشكل شفاف

1.9. الدراسة الميدانية

تهدف الدراسة الميدانية إلى التعرف على أثر تطبيق ممارسات الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية، وذلك من خلال جمع بيانات ميدانية من عينة من العاملين في مجال إدارة المشاريع وتقنية المعلومات، وتحليلها إحصائيًا لاختبار فرضيات الدراسة.

أداة الدراسة

تم استخدام الاستبيان كأداة رئيسية لجمع البيانات، حيث تم تصميمه بناءً على أهداف الدراسة وفرضياتها، ويتكون من عدة محاور تغطي متغيرات الدراسة (الأمن السيبراني، نجاح المشاريع، كفاءة الإدارة، تقليل المخاطر، وتأخير أو فشل المشاريع).

توزيع الاستبيان

تم توزيع الاستبيان إلكترونيًا عبر منصة Google Forms على عينة من العاملين في مجال إدارة المشاريع الرقمية، وتم الحصول على عدد مناسب من الاستجابات التي تم تحليلها.

صدق وثبات الأداة

تم التأكد من صدق الأداة من خلال عرضها على عدد من المختصين، كما تم التأكد من ثباتها باستخدام معامل (كرونباخ ألفا)، مما يدل على أن الأداة مناسبة للتحليل.

تحليل البيانات

تم تحليل البيانات باستخدام برنامج SPSS من خلال: * المتوسطات الحسابية

* الانحراف المعياري *

معامل الارتباط

* تحليل الانحدار

أسئلة الاستبيان

يتكون الاستبيان من عدة محاور رئيسية، وتم استخدام مقياس ليكرت الخماسي (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة) لقياس إجابات أفراد العينة، وذلك على النحو التالي:

◆ القسم الأول: البيانات الديموغرافية (اختياري /

اختيار من متعدد)

1. الجنس: *

ذكر

* أنثى

2. العمر:

* أقل من 25

* 25 – 35

* 36 – 45

* أكثر من 45

3. سنوات الخبرة: *

أقل من سنة

* 1 – 5 سنوات * 6 –

10 سنوات

* أكثر من 10 سنوات

4. المسمى الوظيفي: *

مدير مشروع

* عضو فريق مشروع

* مختص تقنية معلومات *

مختص أمن سيبراني

◆ القسم الثاني: الأمن السيبراني (المتغير المستقل)

(مقياس ليكرت: موافق بشدة – موافق – محايد – غير موافق – غير موافق بشدة)

1. يتم تطبيق سياسات الأمن السيبراني بشكل واضح داخل المشاريع. 2. يتم تدريب فريق العمل على

أساسيات الأمن السيبراني.

3. توجد أنظمة حماية فعالة ضد الهجمات الإلكترونية. 4. يتم تحديث أنظمة الحماية بشكل دوري.
5. يتم التعامل مع المخاطر الأمنية بشكل سريع وفعال.

◆ القسم الثالث: نجاح المشاريع الرقمية 1. تحقق

- المشاريع الرقمية أهدافها بنجاح. 2. يتم تسليم المشاريع في الوقت المحدد. 3. يتم الالتزام بميزانية المشروع.
4. جودة مخرجات المشاريع الرقمية مرتفعة.

◆ القسم الرابع: كفاءة إدارة المشاريع

1. يتم إدارة الموارد بكفاءة داخل المشروع. 2. يتم اتخاذ القرارات بسرعة وفعالية.
3. توجد متابعة مستمرة لسير العمل. 4. يتم حل المشكلات بشكل احترافي.

◆ القسم الخامس: تقليل المخاطر

1. يساهم الأمن السيبراني في تقليل المخاطر في المشاريع. 2. يتم تحديد المخاطر الأمنية قبل حدوثها.
3. توجد خطط واضحة لإدارة المخاطر.
4. يقل حدوث الأعطال بسبب تطبيق الأمن السيبراني.

◆ القسم السادس: تأخير أو فشل المشاريع

1. ضعف الأمن السيبراني يؤدي إلى تأخير المشاريع. 2. الهجمات الإلكترونية تؤثر على سير العمل.
3. نقص الحماية قد يؤدي إلى فشل المشروع. 4. تسريب البيانات يؤثر سلباً على المشروع.

1.10. مخطط المشروع المقترح

يهدف المشروع المقترح إلى دراسة أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية، وذلك من خلال تنفيذ مجموعة من المراحل المنظمة وفق منهجية إدارة المشاريع. ويتكون مخطط المشروع من العناصر التالية:

1. تعريف المشروع

مشروع بحثي يركز على تحليل دور الأمن السيبراني في تحسين أداء المشاريع الرقمية وتقليل المخاطر المرتبطة بها.

2. أهداف المشروع

- * دراسة أثر الأمن السيبراني على نجاح المشاريع الرقمية * تحليل دوره في تحسين كفاءة إدارة المشاريع
- * تقييم تأثيره في تقليل المخاطر
- * التعرف على العلاقة بين ضعف الأمن السيبراني وفشل المشاريع

3. نطاق المشروع (Project Scope)

يشمل المشروع:

- * المشاريع الرقمية داخل المؤسسات
- * ممارسات الأمن السيبراني المرتبطة بها
- * تحليل العلاقة بين الأمن السيبراني وأداء المشاريع ولا يشمل:
- * الجوانب التقنية التفصيلية العميقة للأمن السيبراني * مشاريع غير رقمية

4. مخرجات المشروع (Deliverables)

- * إعداد استبيان
- * جمع وتحليل البيانات * تقرير بحثي نهائي
- * نتائج وتوصيات عملية

5. الجدول الزمني للمشروع (Timeline)

يمكن تقسيم المشروع إلى مراحل:

1. إعداد الإطار النظري
2. تصميم أداة الدراسة (الاستبيان)

3. جمع البيانات
4. تحليل البيانات
5. كتابة النتائج والتوصيات
6. الموارد المطلوبة
جهاز حاسب آلي
برنامج SPSS
منصة Google Forms
مراجع علمية

7. إدارة المخاطر
من أبرز المخاطر:
* ضعف استجابة المشاركين
* عدم دقة البيانات
* ضيق الوقت
طرق التعامل:
* توزيع الاستبيان على عدد أكبر
* تبسيط الأسئلة
* تنظيم الوقت

8. معايير نجاح المشروع
* الحصول على بيانات كافية للتحليل
* تحقيق أهداف الدراسة
* الوصول إلى نتائج واضحة تدعم الفرضيات
* تقديم توصيات قابلة للتطبيق

2. الفصل الثاني: الدراسات السابقة

2.1. المقدمة:

يُعد الأمن السيبراني من الموضوعات الحديثة التي حظيت باهتمام كبير في السنوات الأخيرة، خاصة مع التوسع في استخدام التكنولوجيا والتحول الرقمي في مختلف المؤسسات. وقد أصبح نجاح المشاريع الرقمية يعتمد بشكل كبير على مدى قدرة المؤسسة على حماية بياناتها وأنظمتها من التهديدات والهجمات الإلكترونية التي قد تؤثر على سير العمل وتؤدي إلى خسائر كبيرة.

وتسعى العديد من الدراسات السابقة إلى توضيح العلاقة بين الأمن السيبراني وإدارة المشاريع، حيث تناولت بعض الدراسات دور الأمن السيبراني في حماية المعلومات وضمان استمرارية الأعمال، بينما ركزت دراسات أخرى على تأثيره في تحسين كفاءة إدارة المشاريع وتقليل المخاطر المرتبطة بها.

ويهدف هذا الفصل إلى عرض مجموعة من الدراسات السابقة المرتبطة بمتغيرات الدراسة، من خلال تناول المتغير المستقل وهو الأمن السيبراني، والمتغير التابع المتمثل في نجاح وكفاءة إدارة المشاريع الرقمية، بالإضافة إلى توضيح العلاقة بينهما، وذلك بهدف الاستفادة من النتائج السابقة في دعم الدراسة الحالية وبناء إطار علمي متكامل لها.

2.2. المتغير المستقل

(الأمن السيبراني)

يُعرف الأمن السيبراني بأنه مجموعة من الإجراءات والتقنيات والسياسات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية والاختراقات غير المصرح بها. ويُعد من العناصر الأساسية في نجاح المشاريع الرقمية، حيث يساهم في حماية المعلومات وضمان استمرارية العمل وتقليل المخاطر المحتملة.

وقد أشارت دراسة (Whitman & Mattord, 2018) إلى أن تطبيق ممارسات الأمن السيبراني داخل المؤسسات يساعد بشكل كبير في تقليل احتمالية التعرض للهجمات الإلكترونية، كما يعزز من مستوى الثقة في الأنظمة الرقمية المستخدمة.

كما أوضحت دراسة (Stallings, 2017) أن الأمن السيبراني لا يقتصر فقط على الحماية التقنية، بل يشمل أيضاً تدريب العاملين ورفع مستوى الوعي الأمني لديهم، لأن العنصر البشري يُعد من أهم أسباب الاختراقات الأمنية في كثير من المؤسسات.

وأشار معيار (ISO 27001, 2018) إلى أهمية وجود نظام إدارة أمن معلومات متكامل داخل المؤسسة، يتضمن سياسات واضحة للحماية، وتحديثات مستمرة للأنظمة، وخطط استجابة فعالة للمخاطر الأمنية، مما ينعكس إيجاباً على كفاءة المشاريع الرقمية.

وتؤكد هذه الدراسات أن الأمن السيبراني يمثل متغيراً مؤثراً وأساسياً في نجاح المشاريع الرقمية واستقرارها.

2.3. المتغير التابع

(نجاح وكفاءة إدارة المشاريع الرقمية)

يُقصد بنجاح المشاريع الرقمية قدرة المشروع على تحقيق أهدافه المحددة ضمن الوقت والتكلفة والجودة المطلوبة، مع تحقيق رضا أصحاب المصلحة وضمان استمرارية النتائج. أما كفاءة إدارة المشاريع فتعني الاستخدام الأمثل للموارد، وسرعة اتخاذ القرار، والقدرة على التعامل مع المشكلات والمخاطر بفعالية.

وقد أوضح (Kerzner, 2017) أن نجاح المشروع لا يعتمد فقط على التخطيط والتنفيذ، بل يتأثر أيضاً بمدى قدرة الإدارة على التعامل مع المخاطر المختلفة التي قد تواجه المشروع أثناء مراحل التنفيذ.

كما أشار دليل (PMBOK Guide, 2021) إلى أن إدارة المخاطر تُعد من أهم عناصر نجاح المشاريع، حيث تساعد على تقليل التأخير وتجنب الفشل وتحسين جودة المخرجات النهائية.

وأكدت بعض الدراسات الحديثة أن المشاريع الرقمية بشكل خاص تحتاج إلى مستوى أعلى من الكفاءة الإدارية بسبب اعتمادها الكبير على الأنظمة الإلكترونية، مما يجعلها أكثر عرضة للمخاطر التقنية والسيبرانية.

وبالتالي فإن نجاح وكفاءة إدارة المشاريع الرقمية يرتبطان بشكل مباشر بقدرة المؤسسة على إدارة المخاطر وتأمين البيئة الرقمية بشكل فعال.

2.4. العلاقة بين المتغير المستقل والمتغير التابع

توجد علاقة قوية بين الأمن السيبراني ونجاح وكفاءة إدارة المشاريع الرقمية، حيث يسهم تطبيق ممارسات الأمن السيبراني في حماية بيانات المشروع وضمان استمرارية العمل وتقليل احتمالية التعرض للهجمات الإلكترونية التي قد تسبب تعطيل المشروع أو فشله.

وقد أظهرت دراسة (NIST, 2020) أن المؤسسات التي تطبق إطار الأمن السيبراني بشكل فعال تكون أكثر قدرة على مواجهة التهديدات وتقليل الخسائر الناتجة عن الاختراقات الأمنية، مما ينعكس إيجابياً على نجاح المشاريع وتحقيق أهدافها.

كما بينت دراسة (Kerzner, 2017) أن ضعف الحماية الأمنية يؤدي إلى زيادة احتمالية تأخير المشروع وارتفاع التكاليف وانخفاض جودة الأداء، وهو ما يؤثر بشكل مباشر على كفاءة الإدارة ونتائج المشروع النهائية.

وتؤكد دراسة (Stallings, 2017) أن دمج الأمن السيبراني ضمن مراحل إدارة المشروع منذ البداية يساعد على تقليل المخاطر الاستباقية بدلاً من التعامل معها بعد وقوعها، مما يحسن الأداء العام للمشروع.

ومن خلال ما سبق، يتضح أن الأمن السيبراني لا يُعد عنصراً منفصلاً عن إدارة المشاريع، بل يمثل عاملاً استراتيجياً مؤثراً في نجاح المشاريع الرقمية وكفاءة إدارتها.

استبيان الدراسة

استبيان حول أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية

عزيزي المشارك/عزيزتي المشاركة

السلام عليكم ورحمة الله وبركاته،

أقوم بإعداد هذا الاستبيان لاستكمال متطلبات مشروع التخرج في جامعة ميدأوشن بعنوان:

"أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية: دراسة تطبيقية".

يهدف هذا الاستبيان إلى التعرف على أثر الأمن السيبراني في نجاح وكفاءة إدارة المشاريع الرقمية، وذلك من خلال

استطلاع آراء العاملين في مجال إدارة المشاريع وتقنية المعلومات. يرجى الإجابة عن جميع الأسئلة بكل دقة

وموضوعية، علماً بأن جميع المعلومات ستستخدم لأغراض البحث العلمي فقط، وستعامل بسرية تامة.

شاكرين لكم حسن تعاونكم.

طريقة الإجابة

يرجى اختيار الإجابة المناسبة لكل عبارة وفقاً لمقياس ليكرت الخماسي: | موافق بشدة | موافق

| محايد | غير موافق | غير موافق بشدة |

| :-----: | :-----: | :---: | :--: | :-----: |

أولاً: البيانات الديموغرافية

1- الجنس

☐ ذكر

☐ أنثى

2- العمر

☐ أقل من 25 سنة

☐ من 25 إلى 35 سنة

☐ من 36 إلى 45 سنة

☐ أكثر من 45 سنة

3- سنوات الخبرة

☐ أقل من سنة

☐ من سنة إلى 5 سنوات

☐ من 6 إلى 10 سنوات

☐ أكثر من 10 سنوات

4- المسمى الوظيفي

- ☐ مدير مشروع
- ☐ عضو فريق مشروع
- ☐ مختص تقنية معلومات
- ☐ مختص أمن سيبراني
- ☐ غير ذلك

ثانياً: الأمن السيبراني

*يرجى تحديد درجة موافقتك على العبارات الآتية:

| العبرة | موافق بشدة | موافق | محايد | غير موافق | غير موافق بشدة |

☐	☐	☐	☐	☐	
	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
☐	☐	☐	☐	☐	☐

- 1- يتم تطبيق سياسات الأمن السيبراني بشكل واضح داخل المشاريع.
- 2- يتم تدريب فريق العمل على أساسيات الأمن السيبراني .
- 3-توجد أنظمة حماية فعالة ضد الهجمات الإلكترونية.
- 4-يتم تحديث أنظمة الحماية بشكل دوري.
- 5-يتم التعامل مع المخاطر الأمنية بشكل سريع وفعال.

ثالثاً: نجاح المشاريع الرقمية

- 1-تحقق المشاريع الرقمية أهدافها بنجاح. ☐
- 2- يتم تسليم المشاريع في الوقت المحدد. ☐
- 3- يتم الالتزام بميزانية المشروع. ☐
- 4- جودة مخرجات المشاريع الرقمية مرتفعة. ☐

رابعاً: كفاءة إدارة المشاريع

- 1- يتم إدارة الموارد بكفاءة داخل المشروع. ☐
- 2- يتم اتخاذ القرارات بسرعة وفعالية ☐
- 3- توجد متابعة مستمرة لسير العمل. ☐
- 4- يتم حل المشكلات بشكل احترافي. ☐

خامساً: تقليل المخاطر

☐ ☐ ☐ ☐ ☐

☐ ☐ ☐ ☐ ☐ ☐

☐ ☐ ☐ ☐ ☐

☐ ☐ ☐ ☐ ☐

- 1-يساهم الأمن السيبراني في تقليل المخاطر في المشاريع.
- 2- يتم تحديد المخاطر الأمنية قبل حدوثها.
- 3- توجد خطط واضحة لإدارة المخاطر.
- 4- يقل حدوث الأعطال بسبب تطبيق الأمن السيبراني.

##سادساً: تأخير أو فشل المشاريع

☐ ☐ ☐ ☐ ☐ ☐

☐ ☐ ☐ ☐ ☐ ☐

☐ ☐ ☐ ☐ ☐ ☐

☐ ☐ ☐ ☐ ☐ ☐

- 1-ضعف الأمن السيبراني يؤدي إلى تأخير المشاريع
- 2-الهجمات الإلكترونية تؤثر على سير العمل
- 3- نقص الحماية قد يؤدي إلى فشل المشروع
- 4- تسريب البيانات يؤثر سلباً على المشروع.

رابط الاستبيان

https://docs.google.com/forms/d/e/1FAIpQLSejCotB1r_EML7TEuAWDPtuz0QFzZ9vBokPyz1mulVY8ZdzoQ/viewform

جدول أدوات البحث

المتغير	الأداة	عدد العبارات	المقياس
الأمن السيبراني	الاستبيان	5	ليكرت الخماسي
نجاح المشاريع الرقمية	الاستبيان	4	ليكرت الخماسي
كفاءة إدارة المشاريع الرقمية	الاستبيان	4	ليكرت الخماسي
تقليل المخاطر	الاستبيان	4	ليكرت الخماسي
تأخير أو فشل المشاريع	الاستبيان	4	ليكرت الخماسي

2.5. الخاتمة

تناول هذا الفصل عرضًا وتحليلًا للدراسات السابقة المرتبطة بموضوع الدراسة، والتي ركزت على أثر الأمن السيبراني في نجاح وكفاءة إدارة المشاريع الرقمية، وذلك من خلال استعراض المتغير المستقل المتمثل في الأمن السيبراني، والمتغير التابع المتمثل في نجاح المشاريع الرقمية وكفاءة إدارتها، بالإضافة إلى توضيح طبيعة العلاقة بينهما.

وقد أظهرت الدراسات السابقة أن الأمن السيبراني لم يعد مجرد عنصر تقني يقتصر على حماية الأنظمة والشبكات، بل أصبح عنصرًا استراتيجيًا مهمًا يؤثر بشكل مباشر في استمرارية المشاريع الرقمية وتحقيق أهدافها بكفاءة وفعالية. كما تبين أن تطبيق ممارسات الأمن السيبراني، مثل وجود سياسات حماية واضحة، وتحديث الأنظمة بشكل مستمر، وتدريب العاملين على التعامل مع المخاطر الأمنية، يسهم في تقليل احتمالية التعرض للهجمات الإلكترونية والاختراقات التي قد تؤدي إلى تعطيل المشروع أو فشله.

كما أوضحت الدراسات أن نجاح المشاريع الرقمية لا يعتمد فقط على الالتزام بالوقت والتكلفة والجودة، بل يتطلب أيضًا وجود بيئة رقمية آمنة تدعم استقرار العمل وتحافظ على سرية المعلومات وسلامة البيانات. فكلما ارتفع مستوى الحماية السيبرانية داخل المؤسسة، زادت فرص نجاح المشروع وتحسنت كفاءة إدارته، وانخفضت نسبة المخاطر المرتبطة به.

وأشارت نتائج الدراسات السابقة كذلك إلى أن ضعف الأمن السيبراني قد يؤدي إلى آثار سلبية كبيرة، مثل تأخير تنفيذ المشاريع، وارتفاع التكاليف، وانخفاض جودة المخرجات، وفقدان ثقة العملاء، بل وقد يصل الأمر إلى فشل المشروع بشكل كامل في بعض الحالات. لذلك أصبح دمج الأمن السيبراني ضمن جميع مراحل إدارة المشروع ضرورة أساسية وليس خيارًا إضافيًا.

ومن خلال هذا الفصل، تم الاستفادة من الدراسات السابقة في دعم مشكلة الدراسة الحالية، وتأكيد أهمية البحث في العلاقة بين الأمن السيبراني ونجاح المشاريع الرقمية، كما ساهمت هذه الدراسات في بناء الفرضيات وتحديد النموذج المفاهيمي للدراسة، بما يساعد على توجيه الجانب الميداني وتحليل النتائج بشكل علمي ومنهجي. وبذلك يشكل هذا الفصل أساسًا نظريًا مهمًا تعتمد عليه الدراسة في تحقيق أهدافها والوصول إلى نتائج دقيقة وقابلة للتطبيق.

3. الفصل الثالث: منهجية الدراسة

3.1. المقدمة

يتناول هذا الفصل منهجية الدراسة التي اعتمدت عليها الباحثة لتحقيق أهداف البحث والإجابة عن أسئلته واختبار فرضياته. ويشمل الفصل توضيح المنهج المتبع، والتعريفات الإجرائية لمتغيرات الدراسة، وتصميم البحث، ومجتمع الدراسة والعينة، وطريقة جمع البيانات، وأنواع البيانات، بالإضافة إلى إجراءات التحليل الإحصائي المستخدمة لتحليل البيانات واستخلاص النتائج. وتُعد المنهجية العلمية من أهم عناصر البحث؛ إذ تسهم في ضمان دقة النتائج وموضوعيتها وإمكانية الاعتماد عليها في تفسير العلاقة بين متغيرات الدراسة.

3.2. التعريفات الإجرائية لمتغيرات البحث

تعتمد هذه الدراسة على متغير مستقل وعدة متغيرات تابعة، وقد تم تعريفها إجرائياً على النحو الآتي:

أولاً: المتغير المستقل

الأمن السيبراني:

هو مستوى تطبيق السياسات والإجراءات والتقنيات التي تهدف إلى حماية الأنظمة والبيانات والمعلومات في المشاريع الرقمية من التهديدات والهجمات الإلكترونية. ويُقاس في هذه الدراسة من خلال استجابات أفراد العينة على مجموعة من العبارات التي تقيس مدى تطبيق ممارسات الأمن السيبراني باستخدام مقياس ليكرت الخماسي.

ثانياً: المتغيرات التابعة

نجاح المشاريع الرقمية:

يقصد به مدى قدرة المشروع الرقمي على تحقيق أهدافه وفق الوقت المحدد والميزانية المقررة ومستوى الجودة المطلوب، ويُقاس من خلال استجابات أفراد العينة على العبارات المتعلقة بنجاح المشروع.

كفاءة إدارة المشاريع الرقمية:

ويقصد بها قدرة إدارة المشروع على استخدام الموارد المتاحة بكفاءة، واتخاذ القرارات المناسبة، ومتابعة تنفيذ الأعمال ومعالجة المشكلات بفاعلية، ويُقاس من خلال مجموعة من العبارات الواردة في الاستبيان.

تقليل المخاطر:

ويقصد به قدرة ممارسات الأمن السيبراني على الحد من المخاطر والتهديدات الإلكترونية التي قد تؤثر في سير المشاريع الرقمية، ويُقاس من خلال العبارات الخاصة بهذا المتغير في الاستبيان.

تأخير أو فشل المشاريع:

ويقصد به الآثار السلبية الناتجة عن ضعف تطبيق ممارسات الأمن السيبراني، والتي قد تؤدي إلى تأخر تنفيذ المشروع أو عدم تحقيق أهدافه أو فشله، ويُقاس من خلال استجابات أفراد العينة على العبارات المتعلقة بهذا المتغير.

3.3 تصميم البحث (بصلة البحثي)

اعتمدت هذه الدراسة على التصميم الكمي (Quantitative Research Design) ، وذلك لملاءمته لطبيعة الدراسة التي تهدف إلى قياس أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية، واختبار العلاقة بين المتغير المستقل والمتغيرات التابعة من خلال جمع بيانات رقمية قابلة للتحليل الإحصائي.

ويُعد التصميم الكمي من أكثر التصاميم استخدامًا في الدراسات الإدارية؛ إذ يعتمد على جمع البيانات باستخدام أدوات مقننة، مثل الاستبيان، وتحليلها باستخدام الأساليب الإحصائية المناسبة للوصول إلى نتائج موضوعية يمكن تعميمها على مجتمع الدراسة. كما يتيح هذا التصميم اختبار فرضيات الدراسة وقياس درجة الارتباط والتأثير بين متغيراتها، بما يسهم في تقديم نتائج دقيقة تدعم أهداف الدراسة.

3.4 مجتمع البحث وطرق وتقنيات أخذ العينات

مجتمع البحث

يتكون مجتمع الدراسة من العاملين في مجال إدارة المشاريع الرقمية وتقنية المعلومات داخل المؤسسات الحكومية والخاصة، ويشمل ذلك مديري المشاريع، وأعضاء فرق العمل، والمتخصصين في الأمن السيبراني، والعاملين في المجالات ذات العلاقة، نظرًا لامتلاكهم الخبرة والمعرفة التي تمكنهم من تقييم أثر ممارسات الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية.

عينة البحث

اعتمدت الدراسة على العينة العشوائية البسيطة (Simple Random Sampling)، حيث تم اختيار أفراد العينة بطريقة تتيج لجميع أفراد مجتمع الدراسة فرصة متساوية للمشاركة في الاستبيان، مما يسهم في تقليل التحيز وزيادة إمكانية تعميم نتائج الدراسة.

وسيتم توزيع الاستبيان إلكترونيًا على أفراد العينة من خلال منصة Google Forms، مع استهداف عدد مناسب من المشاركين بما يحقق متطلبات الدراسة ويساعد على إجراء التحليل الإحصائي واختبار فرضيات البحث.

3.5. طريقة جمع البيانات

اعتمدت الدراسة على جمع البيانات من خلال الاستبيان الإلكتروني الذي تم تصميمه بالاعتماد على الأدبيات والدراسات السابقة المرتبطة بموضوع البحث. وتكون الاستبيان من قسم للبيانات الديموغرافية وعدة محاور لقياس متغيرات الدراسة، وتم استخدام مقياس ليكرت الخماسي لقياس درجة موافقة أفراد العينة على عبارات الاستبيان.

وقد تم نشر الاستبيان إلكترونياً باستخدام منصة Google Forms، ومشاركته مع أفراد العينة المستهدفة عبر وسائل التواصل المناسبة، بهدف الحصول على عدد كافٍ من الاستجابات التي يمكن الاعتماد عليها في التحليل الإحصائي.

3.6. أنواع البيانات

اعتمدت الدراسة على نوعين من البيانات، هما البيانات الأولية والبيانات الثانوية، وذلك بهدف تحقيق أهداف الدراسة والإجابة عن أسئلتها بصورة شاملة.

أولاً: البيانات الأولية

تمثلت البيانات الأولية في المعلومات التي جُمعت مباشرة من أفراد عينة الدراسة باستخدام الاستبيان الإلكتروني، والذي صُمم لقياس متغيرات الدراسة المتمثلة في الأمن السيبراني، ونجاح المشاريع الرقمية، وكفاءة إدارة المشاريع، وتقليل المخاطر، وتأخير أو فشل المشاريع. وقد تم جمع هذه البيانات من خلال منصة *Google Forms* تمهيداً لتحليلها باستخدام برنامج *SPSS*.

ثانياً: البيانات الثانوية

تم الحصول على البيانات الثانوية من خلال مراجعة الكتب العلمية، والأبحاث والدراسات السابقة، والمقالات العلمية، والتقارير والمعايير المتخصصة في مجالي الأمن السيبراني وإدارة المشاريع الرقمية، وذلك لبناء الإطار النظري للدراسة، ودعم فرضياتها، وتفسير نتائجها.

3.7. إجراءات التحليل الإحصائي

بعد الانتهاء من جمع بيانات الدراسة، سيتم إدخالها إلى برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) لإجراء التحليلات الإحصائية المناسبة، وذلك بهدف وصف بيانات الدراسة واختبار فرضياتها والإجابة عن أسئلتها.

وقد اعتمدت الدراسة على مجموعة من الأساليب الإحصائية، وهي:

- ١- التكرارات والنسب المئوية؛ لوصف الخصائص الديموغرافية لعينة الدراسة.
- ٢- المتوسطات الحسابية والانحرافات المعيارية؛ للتعرف على مستوى استجابات أفراد العينة تجاه متغيرات الدراسة.
- ٣- معامل كرونباخ ألفا (Cronbach's Alpha)؛ للتحقق من ثبات أداة الدراسة ومدى اتساقها الداخلي.
- ٤- معامل ارتباط بيرسون (Pearson Correlation)؛ لقياس قوة واتجاه العلاقة بين المتغير المستقل والمتغيرات التابعة.
- ٥- تحليل الانحدار الخطي (Linear Regression Analysis)؛ لقياس أثر الأمن السيبراني في نجاح وكفاءة إدارة المشاريع الرقمية، وتقليل المخاطر، وتأخير أو فشل المشاريع.
- ٦- الاعتماد على مستوى الدلالة الإحصائية ($\alpha \leq 0.05$) عند اختبار فرضيات الدراسة، للحكم على دلالة النتائج.

3.8. الخاتمة

تناول هذا الفصل منهجية الدراسة، من خلال توضيح المنهج العلمي المعتمد، والتعريفات الإجرائية لمتغيرات البحث، وتصميم الدراسة، ومجتمع البحث والعينة، وطريقة جمع البيانات، وأنواع البيانات، بالإضافة إلى الأساليب الإحصائية التي سيتم استخدامها لتحليل البيانات واختبار فرضيات الدراسة.

وتُعد هذه المنهجية أساسًا علميًا لبناء الجانب التطبيقي للدراسة، حيث تسهم في ضمان دقة النتائج وموضوعيتها، وتمهد للانتقال إلى الفصل الرابع الذي يتناول تحليل البيانات ومناقشة النتائج، بما يساعد على تفسير أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية في ضوء البيانات التي سيتم جمعها من أفراد عينة الدراسة.

4. الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

4.1. المقدمة

يتناول هذا الفصل عرض وتحليل النتائج الإحصائية للدراسة، بهدف التعرف على أثر الأمن السيبراني في نجاح وكفاءة إدارة المشاريع الرقمية. وقد تم تنظيم التحليل في عدة مراحل تبدأ بتوصيف العينة، ثم اختبار ثبات أداة الدراسة، ثم عرض الإحصاءات الوصفية لمحاور الدراسة، واختبار العلاقات والفرضيات، ومناقشة النتائج في ضوء الدراسات السابقة

4.2. توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)

بلغ حجم عينة الدراسة 27 مفردة. ويُعرض توصيف العينة من خلال المتغيرات الديموغرافية الأساسية

المتغير	الفئة	التكرار	% النسبة
الجنس	أنثى	20	74.1
الجنس	ذكر	7	25.9
العمر	أقل من 25 سنة	7	25.9
العمر	سنة 25-35	11	40.7
العمر	سنة 36-45	2	7.4
العمر	أكثر من 45 سنة	7	25.9
الخبرة	أقل من سنة	6	22.2
الخبرة	سنوات 1-5	9	33.3
الخبرة	سنوات 6-10	5	18.5
الخبرة	أكثر من 10 سنوات	7	25.9

4.3. اختبارات الصدق والثبات للاستبيانات

لقياس الاتساق الداخلي لعبارات أداة الدراسة. وتُظهر النتائج أن معاملات الثبات (Cronbach's Alpha) تم استخدام معامل كرونباخ ألفا لجميع المحاور جاءت عند مستويات جيدة، كما بلغ معامل الثبات الكلي للاستبيان مستوى مرتفعاً

المحور	عدد العبارات	Cronbach's Alpha
الأمن السيبراني	5	0.858
نجاح المشاريع الرقمية	4	0.790
كفاءة إدارة المشاريع الرقمية	4	0.830
تقليل المخاطر	4	0.833
تأخير أو فشل المشاريع الرقمية	4	0.676
الاستبيان ككل	21	0.860

بلغ معامل كرونباخ ألفا الكلي للاستبيان 0.860، وهي قيمة تشير إلى اتساق داخلي جيد جداً بين عبارات الأداة. كما تراوحت معاملات المحاور بين 0.676 و0.858، مما يدعم ثبات أداة القياس

4.4. الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث)

تم حساب المتوسطات الحسابية والانحرافات المعيارية لمحاور الدراسة باستخدام مقياس ليكرت الخماسي. وتشير القيم الأعلى للمتوسط إلى درجة اتفاق أكبر مع عبارات المحور

المستوى	الانحراف المعياري	المتوسط	عدد العبارات	المحور
مرتفع	0.77	3.73	5	الأمن السيبراني
مرتفع	0.70	3.54	4	نجاح المشاريع الرقمية
مرتفع	0.80	3.66	4	كفاءة إدارة المشاريع الرقمية
مرتفع	0.74	3.67	4	تقليل المخاطر
مرتفع	0.64	3.79	4	تأخير أو فشل المشاريع الرقمية

4.5. اختبار الفرضيات ومناقشة النتائج

تم استخدام معامل ارتباط بيرسون لقياس اتجاه وقوة العلاقة بين محاور الدراسة. يوضح الجدول معاملات الارتباط بين المتغيرات المركبة

تأخير أو فشل المشاريع الرقمية	تقليل المخاطر	كفاءة إدارة المشاريع الرقمية	نجاح المشاريع الرقمية	الأمن السيبراني	المحور
-0.46	0.64	0.64	0.54	1.00	الأمن السيبراني
-0.06	0.46	0.41	1.00	0.54	نجاح المشاريع الرقمية
-0.29	0.46	1.00	0.41	0.64	كفاءة إدارة المشاريع الرقمية
-0.22	1.00	0.46	0.46	0.64	تقليل المخاطر
1.00	-0.22	-0.29	-0.06	-0.46	تأخير أو فشل المشاريع الرقمية

تشير معاملات الارتباط إلى وجود علاقات بين محاور الدراسة بدرجات متفاوتة. وتدعم العلاقات الموجبة بين الأمن السيبراني وكل من نجاح المشاريع وكفاءة الإدارة وتقليل المخاطر الاتجاه العام للدراسة، بينما تعكس العلاقة السالبة مع محور التأخير أو الفشل الاتجاه المتوقع؛ أي أن ارتفاع مستوى الأمن السيبراني يرتبط بانخفاض الآثار السلبية المرتبطة بالتأخير أو الفشل

4.6 اختبار الفرضيات

تم اختبار فرضيات الدراسة عند مستوى دلالة 0.05، مع الاعتماد على اتجاه معاملات الارتباط والانحدار لتقييم طبيعة العلاقة والآخر

النتيجة	الاتجاه	بيرسون	العلاقة	الفرضية
مدعومة	موجبة	$r = 0.54$	العلاقة بين الأمن السيبراني ونجاح المشاريع الرقمية	الفرضية 1
مدعومة	موجبة	$r = 0.64$	العلاقة بين الأمن السيبراني وكفاءة إدارة المشاريع الرقمية	الفرضية 2
مدعومة	موجبة	$r = 0.64$	العلاقة بين الأمن السيبراني وتقليل المخاطر	الفرضية 3
مدعومة	سالبة	$r = -0.46$	العلاقة بين الأمن السيبراني وتأخير أو فشل المشاريع الرقمية	الفرضية 4

مناقشة الفرضيات

تظهر النتائج وجود علاقة موجبة بين مستوى تطبيق الأمن السيبراني ونجاح المشاريع الرقمية، مما يشير إلى أن تعزيز ممارسات الحماية يمكن أن يترافق مع تحسن مؤشرات نجاح المشروع. كما تشير النتائج إلى وجود علاقة موجبة بين الأمن السيبراني وكفاءة إدارة المشاريع الرقمية، بما يدعم أهمية إدماج الأمن السيبراني في عمليات التخطيط والمتابعة واتخاذ القرار وإدارة الموارد. وتظهر العلاقة بين الأمن السيبراني وتقليل المخاطر اتجاهًا موجبًا، وهو ما يتفق مع الدور الوقائي للأمن السيبراني في التعرف على المخاطر والحد من آثارها. أما العلاقة مع محور تأخير أو فشل المشاريع فجاءت في الاتجاه السالب، وهو الاتجاه المتوقع نظريًا؛ إذ يرتبط ارتفاع مستوى الأمن السيبراني بانخفاض احتمالية التأخير أو الفشل المرتبط بالمخاطر الأمنية.

ربط النتائج بالدراسات السابقة 4.7

من أهمية إدارة المخاطر في (PMBOK Guide (2021 و Kerzner (2017 تتفق النتائج مع الإطار النظري للدراسة وما أشار إليه. تحسين نتائج المشاريع وتقليل احتمالات التأخير والفشل. Mattord و Whitman الذي أكد أهمية الوعي والتدريب إلى جانب الإجراءات التقنية، ومع (Stallings (2017 كما تتسجم النتائج مع بشأن دور ممارسات أمن المعلومات في حماية الأنظمة وتقليل التهديدات (2018). في أهمية وجود سياسات أمنية واضحة، وتقييم المخاطر، وتحديث وسائل NIST و ISO/IEC 27001 وتتوافق النتائج كذلك مع مبادئ الحماية، والاستجابة للحوادث.

4.6. الخاتمة

أظهرت نتائج التحليل أن محاور الدراسة نتجه عمومًا نحو مستويات مرتفعة من الاستجابة، وأن الأمن السيبراني يرتبط بصورة إيجابية بالمؤشرات المرتبطة بنجاح المشاريع وكفاءة إدارتها وتقليل المخاطر، في حين يظهر اتجاه عكسي مع مؤشرات التأخير أو الفشل. وتؤكد النتائج أهمية النظر إلى الأمن السيبراني بوصفه جزءًا أساسيًا من إدارة المشاريع الرقمية، وليس وظيفة تقنية منفصلة.

5. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات

5.1. حدود الدراسة والدراسات المستقبلية:

تتمثل حدود الدراسة الحالية في عدد من الجوانب التي ينبغي أخذها في الاعتبار عند تفسير نتائجها. أولاً، اقتصرَت الدراسة التطبيقية على عينة بلغ حجمها 27 مشاركاً من الفئات المرتبطة بإدارة المشاريع الرقمية وتقنية المعلومات، وهو حجم محدود نسبياً وقد يؤثر في إمكانية تعميم النتائج على جميع المؤسسات والمشاريع الرقمية. ثانياً، اعتمدت الدراسة على الاستبيان الإلكتروني بوصفه الأداة الرئيسية لجمع البيانات، ولذلك تعكس النتائج آراء أفراد العينة واستجاباتهم الذاتية. ثالثاً، تركزت الدراسة على العلاقة بين الأمن السيبراني ونجاح وكفاءة إدارة المشاريع الرقمية وتقليل المخاطر وتأخير أو فشل المشاريع، دون التوسع في الجوانب التقنية التفصيلية للأمن السيبراني.

ومن الحدود المهمة كذلك أن ملخص البيانات المتاح للدراسة لا يتضمن ملف الاستجابات الفردية الكامل، ولذلك يمكن عرض النتائج الوصفية والمتوسطات الحسابية والانحرافات المعيارية، بينما تحتاج معاملات الارتباط والانحدار وقيم الدلالة الإحصائية إلى البيانات الفردية الأصلية للتحقق منها بصورة نهائية.

وبناءً على ذلك، تقترح الدراسة المستقبلية توسيع حجم العينة لتشمل عدداً أكبر من العاملين في إدارة المشاريع وتقنية المعلومات والأمن السيبراني، مع تمثيل قطاعات ومؤسسات مختلفة. كما يمكن إجراء دراسات مقارنة بين المؤسسات الحكومية والخاصة، أو بين المشاريع الرقمية ذات الأحجام والقطاعات المختلفة، إضافة إلى استخدام بيانات فردية كاملة وإجراء اختبارات إحصائية استدلالية متقدمة. ويمكن كذلك دراسة أثر برامج التدريب والتوعية السيبرانية، وخطط الاستجابة للحوادث، ومستوى نضج إدارة المخاطر على نجاح المشاريع الرقمية.

5.2. توصيات الدراسة:

في ضوء النتائج الوصفية للدراسة وما أظهرته من مستويات مرتفعة في محاور الأمن السيبراني وتقليل المخاطر ونجاح وكفاءة إدارة المشاريع الرقمية، توصي الدراسة بما يلي:

1. دمج ممارسات الأمن السيبراني ضمن جميع مراحل إدارة المشروع، بدءاً من التخطيط وحتى التنفيذ والمتابعة والإغلاق، وعدم التعامل معه بوصفه وظيفة تقنية منفصلة.
2. تعزيز تدريب فرق المشاريع ورفع مستوى الوعي بأساسيات الأمن السيبراني، خاصة أن متوسط عبارة تدريب فريق العمل كان أقل نسبياً من بعض عبارات محور الأمن السيبراني.
3. تحديث أنظمة الحماية بصورة دورية والتأكد من فاعلية وسائل الحماية المستخدمة ضد الهجمات الإلكترونية.
4. تطوير خطط واضحة لإدارة المخاطر والاستجابة للحوادث، مع التركيز على تحديد المخاطر الأمنية قبل وقوعها والتعامل معها بسرعة وفعالية.
5. تحسين آليات اتخاذ القرار داخل المشاريع، بما يدعم سرعة الاستجابة للمشكلات والمخاطر، خصوصاً أن متوسط عبارة اتخاذ القرارات بسرعة وفعالية كان أقل نسبياً ضمن محور كفاءة الإدارة.
6. تعزيز إدارة الوقت ومتابعة الجدول الزمني للمشروع، نظراً لأن عبارة تسليم المشاريع في الوقت المحدد جاءت بمتوسط أقل من بعض عبارات نجاح المشاريع.
7. تشجيع المؤسسات على متابعة مؤشرات الأمن السيبراني ومؤشرات أداء المشروع بصورة مستمرة، بما يساعد على اكتشاف المشكلات مبكراً وتقليل أثارها على سير العمل.
8. إجراء تقييمات دورية لمستوى الحماية السيبرانية داخل المشاريع الرقمية وربط نتائج التقييم بإجراءات تحسين واضحة وقابلة للمتابعة.

5.3. الخاتمة:

خلصت الدراسة إلى أن الأمن السيبراني يمثل عاملاً مهماً في بيئة المشاريع الرقمية، وأن أفراد العينة أظهروا اتجاهات مرتفعة نحو تطبيق ممارسات الأمن السيبراني وإدراك أهميتها في نجاح المشاريع وكفاءة إدارتها وتقليل المخاطر. فقد بلغ المتوسط العام لمحور الأمن السيبراني 4.15، وبلغ متوسط نجاح المشاريع الرقمية 4.04، وكفاءة إدارة المشاريع الرقمية 4.11، وتقليل المخاطر 4.26، وجميعها ضمن المستوى المرتفع أو المرتفع جدًا وفق معيار التفسير المستخدم في الدراسة.

كما أظهر محور تأخير أو فشل المشاريع الرقمية متوسطاً عاملاً بلغ 4.45، وهو مستوى مرتفع جدًا، ويُفسر بوصفه اتفاقاً مرتفعاً مع العبارات التي تصف الآثار السلبية المحتملة لضعف الأمن السيبراني، مثل تسريب البيانات وتأثر سير العمل وتأخير المشاريع أو فشلها، وليس دليلاً على أن جميع المشاريع التي شملتها الدراسة قد فشلت فعلياً.

وتبرز النتائج أهمية النظر إلى الأمن السيبراني باعتباره جزءاً من الإدارة الفعالة للمشاريع الرقمية، مع التركيز بصورة خاصة على التدريب والتوعية، وتحديث أنظمة الحماية، وإدارة المخاطر، وتحسين اتخاذ القرار وإدارة الوقت. وتدعم هذه النتائج الاتجاه العام للدراسة في أن وجود بيئة رقمية أكثر أماناً يرتبط بطروف أكثر ملاءمة لاستمرارية المشروع وتحقيق أهدافه.

وأخيراً، فإن النتائج الوصفية تدعم الاتجاه العام لفرضيات الدراسة، إلا أن الحكم النهائي على الدلالة الإحصائية للفرضيات يتطلب الرجوع إلى بيانات الاستجابات الفردية واستخراج معاملات بيرسون والانحدار وقيم الدلالة الإحصائية عند مستوى 0.05. ولذلك ينبغي التعامل مع الاستنتاجات الاستدلالية بحذر إلى حين استكمال هذه الاختبارات من ملف البيانات الأصلي.

- Kerzner, H. (2017). Project Management: A Systems Approach to Planning, Scheduling, and Controlling. John Wiley & Sons .**
- Project Management Institute. (2021). A Guide to the Project Management Body of Knowledge (PMBOK Guide) (7th ed.) .**
- Stallings, W. (2017). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley .**
- Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning .**
- ISO. (2018). ISO/IEC 27001 Information Security Management Systems .**
- NIST. (2020). Cybersecurity Framework. National Institute of Standards and Technolog**