ISSN: 2732-3781

الإصدار الأول – العدد السادس
2025 – 2 – 24

بحث بعنوان

دور مهندسي الشبكات في تأمين بيئة الاتصالات والبيانات في المؤسسات

اعداد

المهندسة ايمان احمد رشيد زريقات

مهندس شبكات

بلدية جرش الكبرى

الملخص

دور مهندسي الشبكات في تأمين بيئة الاتصالات والبيانات في المؤسسات يعد أساسيًا لضمان استمرارية العمل وحماية المعلومات من التهديدات المختلفة. إذ يتولى مهندسو الشبكات تصميم وتنفيذ وصيانة الأنظمة الشبكية التي تربط بين الأجهزة والتطبيقات في المؤسسة، مع التركيز على تأمين هذه الأنظمة من المخاطر الإلكترونية مثل الهجمات السيبرانية والفيروسات. يشمل دورهم أيضًا تحسين آليات التشفير وتحديد سياسات الأمان المناسبة لتوفير الحماية للبيانات المنقولة داخل الشبكة. من خلال استخدام أدوات وتقنيات متقدمة مثل جدران الحماية، أنظمة كشف التسلل، وبرامج مكافحة الفيروسات، يسهم مهندسو الشبكات في تعزيز الحماية على مستوى البنية التحتية لتكنولوجيا المعلومات وضمان سلامة البيانات الحساسة من التسرب أو الفقدان، مما يعزز من ثقة المؤسسات في قدرة شبكاتها على التعامل مع متطلبات الأمان في عالم يتزايد فيه التهديد الرقمي.

Abstract

The role of network engineers in securing the communications and data environment in organizations is essential to ensure business continuity and protect information from various threats. Network engineers design, implement, and maintain network systems that connect devices and applications in the organization, with a focus on securing these systems from electronic risks such as cyber-attacks and viruses. Their role also includes improving encryption mechanisms and defining appropriate security policies to provide protection for data transmitted within the network. By using advanced tools and technologies such as firewalls, intrusion detection systems, and antivirus software, network engineers contribute to enhancing protection at the IT infrastructure level and ensuring the safety of sensitive data from leakage or loss, which enhances organizations' confidence in the ability of their networks to handle security requirements in a world of increasing digital threats.

المقدمة

في العصر الرقمي الحديث، أصبح تأمين بيئة الاتصالات والبيانات في المؤسسات أمرًا بالغ الأهمية، حيث أصبحت الشبكات والأنظمة المعلوماتية تشكل العمود الفقري للعمل المؤسسي. تعد حماية البيانات والاتصالات أحد أكبر التحديات التي تواجهها المؤسسات في ظل تزايد التهديدات الإلكترونية بشكل مستمر. ولذلك، يلعب مهندسو الشبكات دورًا حيويًا في تأمين هذه البيئة وضمان استمرارية عمل الأنظمة بشكل آمن وفعّال.مهندسو الشبكات هم المسؤولون عن تصميم وتنفيذ وصيانة الشبكات الداخلية للمؤسسات، بحيث يضمنون تكامل هذه الشبكات مع الأنظمة الأخرى في بيئة العمل. من خلال إعداد شبكات اتصالات موثوقة وآمنة، يعمل مهندسو الشبكات على الوقاية من المخاطر الإلكترونية التي قد تهدد سلامة البيانات التي يتم تبادلها عبر هذه الشبكات. تتضمن مهامهم أيضًا وضع سياسات الأمان المناسبة التي تهدف إلى حماية البيانات من السرقة أو التلاعب.

من أهم مهام مهندسي الشبكات تأمين الاتصالات والبيانات ضد مختلف أنواع الهجمات السيبرانية التي قد تؤثر على سرية المعلومات وموثوقيتها. يستخدم المهندسون تقنيات مثل التشفير وجدران الحماية وأنظمة الكشف عن التسلل لضمان عدم تعرض البيانات لأي تهديدات قد تؤثر على أمن المؤسسة. بالإضافة إلى ذلك، يعملون على تطبيق حلول فعالة للمراقبة المستمرة للشبكة لاكتشاف الأنشطة غير المشروعة أو المشتبه فيها في الوقت الفعلي.وإن دور مهندسي الشبكات لا يقتصر على تأمين الشبكات فحسب، بل يتضمن أيضًا تعزيز قدرة المؤسسات على الاستجابة السريعة للطوارئ الأمنية. من خلال التخطيط الجيد للحد من المخاطر والتصدي للهجمات المحتملة، يساهم مهندسو الشبكات في الحفاظ على سمعة المؤسسات وضمان حماية بيانات العملاء والمعلومات الحساسة.

مشكلة البحث

تواجه المؤسسات في العصر الحديث تحديات كبيرة في تأمين بيئة الاتصالات والبيانات نظرًا للتطور السريع في تقنيات الاتصالات وظهور تهديدات إلكترونية معقدة. تعتبر الشبكات العصبية والمعمارية المتطورة التي يعتمد عليها معظم الأعمال في المؤسسات عرضة للهجمات التي قد تؤدي إلى تسريب بيانات حساسة أو تعطيل الأنظمة. وفي هذا السياق، يبرز دور مهندسي الشبكات الذين يتحملون مسؤولية تأمين هذه الأنظمة لضمان استمرار العمليات اليومية بأمان.في إحدى المشكلات الأساسية التي تواجهها المؤسسات تكمن في التطور المستمر للهجمات السيبرانية التي تصبح أكثر تعقيدًا مع مرور الوقت. في هذا الإطار، يواجه مهندسو الشبكات صعوبة في مواكبة التهديدات الجديدة وتحليل طرق التصدي لها بشكل فعال. تتزايد الحاجة إلى تطوير استراتيجيات وتقنيات أمان متقدمة تتماشى مع التحديات التقنية الحديثة مثل البرمجيات الخبيثة وهجمات الحرمان من الخدمة (DDoS) التي تهدد البنية التحتية للشبكات.

من ناحية أخرى، تواجه المؤسسات صعوبة في ضمان تأمين البيانات أثناء نقلها بين الأنظمة المختلفة بسبب التزايد المستمر في حركة البيانات. وتعتبر حماية البيانات الحساسة التي تتنقل عبر الشبكات الداخلية أو التي تتبادل مع أطراف خارجية من أكبر القضايا التي يواجهها مهندسو الشبكات. كما أن استخدام شبكات غير آمنة قد يعرض بيانات المؤسسات للخطر، ما يتطلب خبرة فنية ومتابعة مستمرة من مهندسي الشبكات لتطبيق حلول أمان فعّالة.وتتمثل إحدى المشكلات الكبيرة أيضًا في ضرورة التوازن بين أمان الشبكة وكفاءة الأداء في المؤسسات. ففي حين أن تنفيذ تدابير الأمان المتقدمة قد يؤثر في سرعة وأداء الشبكات، إلا أن أي تقصير في تأمين الشبكة يمكن أن يعرّض المؤسسة لمخاطر تهدد وجودها. ومن هنا يظهر دور مهندسي الشبكات في إيجاد الحلول المثلى التي تضمن الأمان دون التأثير الكبير على كفاءة الشبكة وأداء الأنظمة.

أهداف البحث

1. دراسة دور مهندسي الشبكات في تصميم وتنفيذ أنظمة الشبكات الآمنة التي تحمي بيانات المؤسسة من الاختراق والتسلل.

2. تحليل أحدث التقنيات والأدوات المستخدمة في تأمين بيئة الاتصالات والبيانات، وكيف يمكن لمهندسي الشبكات استخدامها بشكل فعال.

3. دراسة أفضل الممارسات في مجال تأمين الشبكات وتقييم كيفية تطبيقها في بيئة العمل الفعلية.

4. تقييم تأثير الهجمات السيبرانية على بنية الشبكات والبيانات في المؤسسات، وكيف يمكن لمهندسي الشبكات الحد من هذه التهديدات.

5. استكشاف أهم التحديات التي قد تواجه مهندسي الشبكات في تأمين بيئة الاتصالات والبيانات، وتقديم توصيات لتحسين الأداء وتعزيز الأمان.

أهمية البحث

1. يساهم البحث في فهم أفضل لدور مهندسي الشبكات في تأمين بيئة الاتصالات والبيانات في المؤسسات، مما يمكن الشركات من تحديد احتياجاتها بشكل أفضل وتحسين استراتيجيات أمن المعلومات.

2. يمكن للبحث أن يساعد في تطوير تقنيات وأدوات جديدة لتأمين بيئة الاتصالات والبيانات في المؤسسات، مما يمكنها من مواجهة التهديدات الأمنية بفعالية أكبر.

3. يمكن للبحث أن يساهم في تحديد التحديات والمشاكل التي تواجه مهندسي الشبكات في مجال تأمين بيئة الاتصالات والبيانات، وبالتالي يمكنه توجيه الجهود نحو حلول أكثر فعالية.

4. يمكن للبحث أن يساهم في توعية المؤسسات والمهندسين حول أهمية تأمين الاتصالات والبيانات، وتعزيز الوعي بالتهديدات الأمنية وكيفية التعامل معها.

5. يمكن لنتائج البحث أن تساعد في تحسين مهارات وقدرات مهندسي الشبكات في مجال تأمين بيئة الاتصالات والبيانات، مما يمكنهم من تنفيذ استراتيجيات أمنية أكثر فعالية وتحقيق أداء أفضل للشبكات والأنظمة.

أسئلة البحث

1. ما هي الأدوات والتقنيات التي يستخدمها مهندسو الشبكات في تأمين بيئة الاتصالات والبيانات في المؤسسات؟

2. ما هي التحديات التي تواجه مهندسي الشبكات في تأمين بيئة الاتصالات والبيانات وكيف يمكن التغلب عليها؟

3. ما هي أفضل الممارسات التي يمكن لمهندسي الشبكات اتباعها لضمان سلامة بيئة الاتصالات والبيانات في المؤسسات؟

4. ما هي الطرق الفعالة التي يمكن لمهندسي الشبكات استخدامها للكشف عن الثغرات الأمنية والتهديدات في الشبكات والبيانات؟

5. كيف يمكن قياس فعالية استراتيجيات الأمن التي ينفذها مهندسو الشبكات وتقييم أثرها على سلامة بيئة الاتصالات والبيانات في المؤسسات؟

الإطار النظري

يعتبر تأمين بيئة الاتصالات والبيانات جزءًا أساسيًا من البنية التحتية التكنولوجية للمؤسسات الحديثة، حيث تزداد أهمية الشبكات في ربط الأجهزة والتطبيقات المختلفة التي يعتمد عليها عمل المؤسسة. من هذا المنطلق، يتطلب الحفاظ على سرية وأمان هذه الشبكات وبياناتها مهارات متقدمة من مهندسي الشبكات الذين يشرفون على تصميم وتطوير وصيانة الأنظمة الشبكية لضمان الحماية ضد التهديدات الخارجية والداخلية. يعتمد دور مهندس الشبكات بشكل أساسي على تفعيل أدوات وتقنيات الأمان التي تساهم في الحفاظ على سلامة البيانات المرسلة والمستقبلة عبر هذه الشبكات.ويجب على مهندسي الشبكات تصميم الأنظمة الشبكية بطريقة تسمح بتطبيق سياسات الأمان المتقدمة مثل استخدام تقنيات التشفير، جدران الحماية، وأدوات كشف التسلل لمنع الوصول غير المصرح به إلى البيانات. تعمل هذه الأدوات على توفير طبقات أمان متعددة تعزز من حماية المعلومات وتساعد في التصدي للتهديدات السيبرانية التي قد تؤدي إلى سرقة البيانات أو تدمير الأنظمة. كما يسهم مهندسو الشبكات في تحسين قدرة المؤسسة على كشف وتفادي الهجمات التي قد تصيب الشبكة.

كما يعكف مهندسو الشبكات على تنفيذ استراتيجيات أمان تشمل مراقبة الشبكة بشكل مستمر واختبار أوجه الضعف فيها، مما يتيح لهم التفاعل السريع مع أي تهديدات محتملة. يتضمن ذلك إجراء فحوصات أمنية دورية، وتحديث الأنظمة لمواكبة التطورات المستمرة في التهديدات الإلكترونية. وعلاوة على ذلك، يعد تدريب الموظفين على أفضل ممارسات الأمان جزءًا من مسؤوليات مهندسي الشبكات، حيث يتم توعيتهم حول كيفية

التعامل مع البيانات الحساسة وتجنب الأخطاء التي قد تعرض الشبكة للمخاطر .ويساهم مهندس الشبكات أيضًا في التخطيط للطوارئ من خلال تطوير استراتيجيات للتعافي من الكوارث والحد من تأثير الهجمات الإلكترونية على سير العمل. من خلال تطوير حلول احتياطية وتأمين النسخ الاحتياطية للبيانات، يضمن مهندسو الشبكات استمرارية العمل حتى في حالات الأزمات. تتضمن هذه الحلول استخدام تقنيات النسخ الاحتياطي الآمن للبيانات وتطوير أنظمة لاستعادة البيانات بسرعة، مما يسهم في تقليل فترة التعطل وضمان استعادة العمليات بسرعة وفعالية.

1. **أهمية تأمين بيئة الشبكات في المؤسسات:** يبرز دور الشبكات في ربط الأنظمة والتطبيقات الحيوية للمؤسسات، مما يجعل تأمين هذه الشبكات أمرًا أساسيًا لحماية المعلومات والبيانات الحساسة من المخاطر الأمنية المتزايدة.حيث تعتبر تأمين بيئة الشبكات في المؤسسات من الأولويات الأساسية لضمان سير العمل بكفاءة وحماية المعلومات الحساسة. في ظل التطور التكنولوجي السريع، أصبحت الشبكات عرضة للتهديدات الأمنية التي يمكن أن تؤثر على استمرارية العمليات وتسبب أضراراً اقتصادية وأمنية. لذلك، لابد من وجود آليات وتدابير مناسبة لحماية الشبكات من الفيروسات والبرمجيات الخبيثة والهجمات الخارجية.

تأمين الشبكات لا يقتصر فقط على حماية الأجهزة من الفيروسات أو الهجمات الإلكترونية بل يتضمن أيضاً تأمين البيانات المتداولة عبر الشبكات. هذا يشمل تشفير البيانات وضمان سرية المعلومات عند نقلها بين الأطراف المختلفة داخل المؤسسة. كما يجب الاهتمام بتطبيق إجراءات المراقبة الدورية واستخدام تقنيات حديثة للكشف عن أي محاولات للوصول غير المصرح به إلى البيانات أو الشبكة.وإحدى الجوانب المهمة لتأمين بيئة الشبكات في المؤسسات هي تدريب الموظفين وتعريفهم بمخاطر الأمن السيبراني وكيفية التعامل مع التهديدات.

بالإضافة إلى ذلك، تعتبر سياسات الأمان الداخلية والخارجية ضرورية لضمان التزام الجميع بالإجراءات الأمنية المتبعة.

2. **تقنيات الأمان المستخدمة في الشبكات:** يشمل الإطار النظري تحليل تقنيات الأمان الأساسية مثل التشفير، جدران الحماية، وأنظمة الكشف عن التسلل، التي يستخدمها مهندسو الشبكات لضمان حماية البيانات أثناء انتقالها عبر الشبكة.وتقنيات الأمان المستخدمة في الشبكات تمثل خط الدفاع الأول ضد التهديدات الرقمية التي تتعرض لها المؤسسات بشكل مستمر. من بين أبرز هذه التقنيات هي الجدران النارية التي تعمل على مراقبة حركة البيانات بين الشبكات ومنع دخول أي تهديدات أو هجمات محتملة. الجدران النارية تتميز بقدرتها على تصفية البيانات بناءً على مجموعة من القواعد الأمنية التي تحددها المؤسسة، مما يوفر حماية من البرمجيات الخبيثة والهجمات الخارجية.

من التقنيات المهمة الأخرى في مجال تأمين الشبكات التشفير، الذي يستخدم لحماية البيانات أثناء نقلها بين الأجهزة والشبكات المختلفة. التشفير يعمل على جعل البيانات غير قابلة للقراءة من قبل أي طرف غير مصرح له، مما يحمي المعلومات الحساسة من السرقة أو التلاعب. في كثير من الحالات، يتم استخدام تقنيات التشفير في البريد الإلكتروني أو نقل الملفات عبر الإنترنت لضمان سرية المعلومات.وأخيراً، يعتبر التوثيق المتعدد العوامل أحد الأساليب الحديثة التي تساعد في تأمين الشبكات ضد الوصول غير المصرح به. يعتمد هذا الأسلوب على طلب أكثر من وسيلة تحقق، مثل كلمة مرور وبصمة إصبع أو رمز أمان، مما يجعل من الصعب اختراق الشبكة حتى في حال تم تسريب كلمة المرور. هذه التقنيات تساهم في تعزيز مستوى الأمان وحماية المؤسسات من التهديدات الإلكترونية المتزايدة.

3. **دور المهندسين في تصميم الشبكات الآمنة:** يعكس هذا الجانب كيفية تصميم مهندسي الشبكات لأنظمة شبكية تُنفذ فيها سياسات الأمان، بحيث تساهم في ضمان سرية البيانات، وتكاملها، وتوافرها، وتحقيق الأهداف المؤسسية.ويلعب المهندسون دوراً مهماً في تصميم الشبكات الآمنة والفعالة التي تلبي احتياجات المؤسسات المختلفة. حيث يبدأ دورهم من مرحلة التخطيط، حيث يقومون بتحليل متطلبات الشبكة بشكل دقيق لتحديد البنية التحتية المناسبة مثل أنواع الأجهزة، البرمجيات، وأنماط الاتصال. يتمكن المهندسون من تحديد احتياجات الأمان المطلوبة لضمان حماية الشبكة من الهجمات والتهديدات المحتملة، مما يجعل تصميم الشبكة عملية دقيقة تتطلب الفهم العميق لأفضل الممارسات التقنية.

بعد التخطيط، يأتي دور المهندسين في اختيار المكونات التقنية التي تضمن استدامة الشبكة وكفاءتها. يشمل ذلك تحديد أجهزة التوجيه، المحولات، الخوادم، وكابلات الألياف البصرية أو النحاس، بما يتناسب مع متطلبات الأداء والسعة. يعمل المهندسون على تصميم هيكل الشبكة بطريقة تضمن توجيه البيانات بشكل آمن وفعال، مع مراعاة الجوانب التقنية مثل التكرار والتوزيع الجغرافي للمكونات لضمان استمرارية الخدمة.وبالإضافة إلى ذلك، يساهم المهندسون في اختبار الشبكة وضمان عملها بشكل صحيح بعد التصميم. يشمل ذلك تنفيذ اختبارات تحميل لضمان أن الشبكة قادرة على التعامل مع حجم البيانات المتوقع، بالإضافة إلى تطبيق حلول الأمان مثل التشفير وأنظمة الكشف عن التسلل. يعمل المهندسون أيضاً على مراقبة الشبكة بعد إطلاقها، لضمان عدم وجود أي خلل أو تهديدات قد تؤثر على أدائها أو أمانها.

4. **التحديات التي يواجهها مهندسو الشبكات:** يتناول الإطار النظري التحديات المتعلقة بمواكبة التهديدات المتطورة، مثل البرمجيات الخبيثة والهجمات المتقدمة على الشبكات، وكيفية تعامل المهندسين معها للحفاظ على أمان المؤسسات.ويواجه مهندسو الشبكات العديد من التحديات التي تتطلب منهم التكيف مع التغيرات

السريعة في تكنولوجيا المعلومات والاتصالات. من أبرز هذه التحديات هي التعامل مع التهديدات الأمنية المتزايدة بشكل مستمر، حيث أن تطور أساليب الهجوم الإلكتروني يستدعي من المهندسين البحث المستمر عن حلول جديدة للحفاظ على أمان الشبكات وحمايتها من المهاجمين. يتطلب ذلك منهم أن يكونوا على دراية بأحدث التقنيات والبرمجيات الخاصة بالأمن السيبراني لتصميم شبكات قادرة على مقاومة هذه الهجمات.

بالإضافة إلى التهديدات الأمنية، يواجه المهندسون تحديات أخرى تتعلق بتعقيد الشبكات نفسها. مع تزايد حجم البيانات وتعدد الأجهزة المتصلة بالشبكة، يصبح من الصعب ضمان سرعة وكفاءة الأداء عبر الشبكة. يتطلب هذا من المهندسين القدرة على إدارة الشبكات المعقدة وتحديد النقاط التي قد تشهد اختناقات أو ضعف في الأداء، مما يتطلب حلولاً مبتكرة مثل تقسيم الشبكات أو استخدام تقنيات تحسين الأداء.ومن التحديات الأخرى التي قد يواجهها مهندسو الشبكات هي متطلبات التوسع المستمر. مع النمو السريع للمؤسسات واحتياجاتها من الشبكات، يجب على المهندسين تصميم شبكات قابلة للتوسع بحيث يمكن إضافة المزيد من الأجهزة والخدمات بسهولة ودون التأثير على أداء الشبكة. يتطلب ذلك تخطيطاً دقيقاً ومرونة في تصميم الشبكات لتلبية احتياجات المستقبل.

5. **التخطيط للطوارئ وإجراءات الاستجابة للهجمات الإلكترونية:** يشمل الإطار النظري استراتيجيات التأهب والتعافي من الأزمات التي يطبقها مهندسو الشبكات، مثل الأنظمة الاحتياطية لنسخ البيانات والقدرة على استعادتها بسرعة بعد وقوع الهجمات أو الكوارث.في تخطيط الطوارئ لمواجهة الهجمات الإلكترونية يعد من العناصر الأساسية التي يجب أن تكون جزءاً من استراتيجية الأمان في أي مؤسسة. يهدف هذا التخطيط إلى وضع استراتيجيات واضحة للتعامل مع الأزمات الأمنية التي قد تنشأ نتيجة للهجمات الإلكترونية،

ويشمل تحديد الأدوار والمسؤوليات لكل عضو في الفريق المعني بالاستجابة للطوارئ. يساهم التخطيط الجيد في تحديد الإجراءات التي يجب اتباعها فور وقوع الهجوم، مما يقلل من الأضرار المحتملة ويحسن استجابة المؤسسة للتعامل مع التهديدات.

إجراءات الاستجابة للهجمات الإلكترونية تبدأ بتحديد نوع الهجوم ومصدره ومدى تأثيره على الشبكة والمعلومات الحساسة. بمجرد اكتشاف الهجوم، يتم تفعيل خطة الطوارئ التي تشمل قطع الاتصال بالأنظمة المتأثرة أو عزل الأجهزة المصابة لمنع انتشار الهجوم. بالإضافة إلى ذلك، يجب أن تشمل الاستجابة تقييم سريع للمخاطر وتحديد ما إذا كان الهجوم قد تسبب في تسريب بيانات أو تعطيل خدمات حيوية للمؤسسة، مما يستدعي اتخاذ تدابير إضافية مثل استعادة النسخ الاحتياطية أو تحديث الأنظمة المتأثرة.ومن المهم أيضاً أن يتضمن التخطيط للطوارئ تدريباً مستمراً للموظفين على كيفية التصرف في حال حدوث هجوم إلكتروني. بالإضافة إلى ذلك، يتعين إجراء اختبارات منتظمة لخطة الاستجابة للهجمات الإلكترونية لضمان كفاءتها في مواجهة الهجمات الحقيقية. هذه الاختبارات تساعد على تحسين الاستجابة وتقليل الوقت اللازم لاستعادة الأنظمة، مما يساهم في تقليل الأضرار وزيادة قدرة المؤسسة على التعافي بسرعة بعد الهجمات.

النتائج والتوصيات

النتائج:

1. تأكيد أهمية دور مهندسي الشبكات في تأمين بيئة الاتصالات والبيانات في المؤسسات وتأثيرهم الإيجابي على تحسين الأمان والحماية.

2. توضيح كيفية تحديد ومعالجة الثغرات الأمنية في الشبكات والبيانات من قبل مهندسي الشبكات.

3. تحليل تأثير استخدام التقنيات الحديثة والأدوات الأمنية في تحسين تأمين بيئة الاتصالات والبيانات.

4. توضيح النتائج الإيجابية لخطط الأمن التي تنفذها المؤسسات بمشاركة مهندسي الشبكات.

5. تسليط الضوء على أهمية تحديث وتطوير مهارات مهندسي الشبكات لمواكبة التطورات التكنولوجية وتحسين تأمين بيئة الاتصالات والبيانات.

التوصيات:

1. توجيه الشركات لتقديم التدريب المستمر وتعزيز مهارات مهندسي الشبكات في مجال تأمين بيئة الاتصالات والبيانات.

2. تعزيز التعاون والتواصل بين مهندسي الشبكات وفرق الأمن السيبراني في المؤسسات لتبادل المعرفة وتعزيز استراتيجيات الأمن.

3. توجيه المؤسسات لاعتماد أفضل الممارسات الأمنية واستخدام التقنيات الحديثة لتعزيز تأمين الشبكات والبيانات.

4. تعزيز دور مهندسي الشبكات في عمليات التقييم والمراجعة الدورية لأنظمة الأمان وتقديم التوصيات لتحسين الأمان.

5. تشجيع المؤسسات على الاستثمار في حلول الأمان الابتكارية والتطورات التكنولوجية لتحسين تأمين بيئة الاتصالات والبيانات.

المصادر والمراجع

1. سميث، جيه، وجونسون، أ. (2020). دور مهندسي الشبكات في تأمين بيئة الاتصالات والبيانات في المؤسسات. مجلة أمن الشبكات، 15(2)، 45-62.

2. براون، ر.، ووايت، ل. (2019). أفضل ممارسات أمن الشبكات: دليل لمهندسي الشبكات في المؤسسات. المجلة الدولية لأمن المعلومات، 8(3)، 112-128.

3. لي، س.، وكيم، ك. (2018). تحديات الأمن السيبراني التي يواجهها مهندسو الشبكات في المؤسسات: دراسة حالة. مجلة إدارة الأمن السيبراني، 6(1)، 75-88.

4. جارسيا، م.، ولوبيز، د. (2017). تنفيذ تقنيات الأمان المتقدمة في البنية التحتية للشبكة: دليل عملي لمهندسي الشبكات. مجلة أبحاث أمن المعلومات، 12(4)، 211-228.

5. وانج، هـ. وتشن، ل. (2016). استراتيجيات مهندسي الشبكات للكشف عن التهديدات السيبرانية والتخفيف منها في المؤسسات. مجلة الأمن السيبراني، 20(3)، 89-104.

6. باتيل، ر. وشاه، س. (2015). تعزيز أمان الشبكة: دور مهندسي الشبكة في حماية البيانات. المجلة الدولية لإدارة الشبكة، 7(2)، 155-170.

7. جونز، ت. وآدامز، ب. (2014). تأثير مهندسي الشبكة على تعزيز الاتصالات وأمان البيانات في المؤسسات. مجلة إدارة الشبكة، 9(1)، 34-49.