IRAQI Academic Scientific Journals
العراقية المجلات الأكاديمية العلمية

مجلة جامعة الكوت

ISSN (E): 2616 - 7808 II ISSN (P): 2414 - 7419

js.uokut.edu.iq

k.u.c.j.sci@alkutcollege.edu.iq

عدد خاص - المؤتمر العلمي التاسع للعلوم الإدارية والاقتصادية - 2-3 مايو/ ايار 2026

# مدى إلزام العراق بتطبيق متطلبات الأمن السيبراني وفق المعايير الدولية

م. م. نبأ ساهي جيجان [1]

**المستخلص**

أصبح الأمن السيبراني اليوم من المتطلبات الأساسية لحماية الدول والمؤسسات في ظل التطور التكنولوجي السريع وزيادة الهجمات الإلكترونية التي تستهدف المعلومات الحساسة والأنظمة الحيوية ويعد الأمن السيبراني عنصرًا رئيسيًا في حماية البنية التحتية الرقمية وتأمين البيانات الحكومية والخاصة من الاختراقات والتهديدات الإلكترونية وقد سعى العراق إلى تنظيم هذا المجال من خلال إصدار مجموعة من التشريعات والقوانين، أبرزها قانون جرائم المعلوماتية رقم 56 لسنة 2017، الذي يهدف إلى حماية المعلومات والنظم الإلكترونية ومعاقبة المخالفين إلا أن تطبيق هذه القوانين يواجه تحديات عديدة، منها ضعف البنية التحتية، ونقص الكوادر البشرية المتخصصة، وعدم وجود آليات متابعة ورقابة فعّالة لضمان التنفيذ السليم ويركز هذا البحث على دراسة التشريعات العراقية وتحليل مدى توافقها مع المعايير الدولية للأمن السيبراني، بما في ذلك معايير الأمم المتحدة، والاتحاد الدولي للاتصالات، ومبادئ ISO/IEC 27001" وكما يستعرض البحث التحديات القانونية والتطبيقية التي تعيق الالتزام الفعلي بهذه المعايير، ويقدم توصيات عملية لتعزيز تطبيقها على المستوى الوطني وتشمل هذه التوصيات تطوير التشريعات القائمة، تحسين البنية التحتية الرقمية، وبناء قدرات بشرية متخصصة قادرة على مواجهة التهديدات السيبرانية الحديثة ويسعى البحث إلى دعم جهود حماية المعلومات الوطنية وتعزيز جاهزية العراق لمواجهة المخاطر الإلكترونية، بما يضمن توافق السياسات الوطنية مع المعايير الدولية، وتحقيق مستوى متقدم من الأمن السيبراني يساهم في حماية الدولة والمجتمع وتعزيز ثقة المؤسسات الرقمية في البلاد.

**الكلمات المفتاحية:** الأمن السيبراني، المعايير الدولية، العراق، ISO/IEC 27001

**انتساب الباحث**

[1] كلية القانون، جامعة واسط، العراق، واسط، الكوت، 52001

[1] nabaa211@uowasit.edu.iq

[1] **المؤلف المراسل**

**معلومات البحث**

**تاريخ النشر:** آب 2026

## The Extent of Iraq's Obligation to Implement Cybersecurity Requirements in Accordance with International Standards

**Asst. Lec. Nabaa Sahi Jejan** [1]

**Abstract**

Cybersecurity has become an essential requirement for protecting states and institutions in light of rapid technological development and the increasing number of cyberattacks targeting sensitive information and critical systems It is a key element in safeguarding digital infrastructure and securing governmental and private data from breaches and electronic threats Iraq has attempted to regulate this field by enacting several laws, most notably Cybercrime Law No. 56 of 2017, which aims to protect information systems and penalize offenders However, the practical application of these laws faces significant challenges, including weak digital infrastructure, a shortage of specialized personnel, and the absence of effective monitoring and enforcement mechanisms This study focuses on examining Iraqi legislation and analyzing its alignment with international cybersecurity standards, including the United Nations guidelines, the International Telecommunication Union frameworks, and the ISO/IEC 27001 principles The research also reviews the legal and practical challenges that hinder Iraq's full compliance with these standards and provides practical recommendations to enhance their application at the national level These recommendations include improving existing legislation, strengthening digital infrastructure, and developing specialized human capacities capable of addressing modern cyber threats The study aims to support national efforts to protect information and enhance Iraq's preparedness against electronic risks, ensuring that national policies align with international standards By doing so, it seeks to achieve a higher level of cybersecurity that protects the state and society while building trust in the country's digital institutions.

**Keywords:** Cybersecurity, International standards, Iraq, ISO/IEC 27001.

**Affiliation of Author**

[1] College of Law, Wasit University, Wasit, Al-Kut, Iraq, 52001

[1] nabaa211@uowasit.edu.iq

[1] **Corresponding Author**

**Paper Info.**

**Published:** Aug. 2026

**المقدمة**

مع التطور التكنولوجي السريع واعتماد الدول والمؤسسات على الأنظمة الرقمية في مختلف المجالات، أصبح الأمن السيبراني ضرورة أساسية لحماية المعلومات والبيانات الحساسة فالهجمات الإلكترونية والجرائم المعلوماتية تمثل تهديدًا مباشرًا للبنية التحتية الحيوية للدولة وللمؤسسات الحكومية والخاصة، مما يفرض على الدول الالتزام بالمعايير الدولية للأمن السيبراني لضمان حماية أنظمتها الرقمية.

سعى العراق إلى تنظيم هذا المجال من خلال إصدار تشريعات تهدف إلى حماية المعلومات والنظم الإلكترونية، وأبرزها قانون جرائم المعلوماتية رقم 56 لسنة 2017. ومع ذلك، يواجه العراق تحديات في التطبيق العملي لهذه القوانين، مثل ضعف البنية التحتية، ونقص الكوادر المتخصصة، وعدم وجود آليات متابعة ورقابة فعّالة.

يهدف هذا البحث إلى دراسة التشريعات العراقية الخاصة بالأمن السيبراني وتحليل مدى توافقها مع المعايير الدولية، بما في ذلك معايير الأمم المتحدة والاتحاد الدولي للاتصالات ومبادئ ISO/IEC 27001"و كما يسلط البحث الضوء على التحديات القانونية والتطبيقية التي تحد من الالتزام الفعلي بهذه المعايير، ويقدم توصيات لتعزيز تطبيقها على المستوى الوطني.

يسعى البحث إلى توضيح مدى جاهزية العراق لمواجهة المخاطر السيبرانية الحديثة، والمساهمة في حماية المعلومات الوطنية وتعزيز الثقة في المؤسسات الرقمية، بما يحقق توافق السياسات الوطنية مع المعايير الدولية ويعزز أمن الدولة والمجتمع. إشكالية:

رغم وجود قوانين للأمن السيبراني في العراق، يبقى التساؤل حول مدى التزام الدولة بالمعايير الدولية، وما هي الثغرات القانونية والتطبيقية الموجودة.

الفرضية:

قد يكون التزام العراق بالمعايير الدولية محدودًا بسبب ضعف البنية التحتية، ونقص الكوادر المتخصصة، وعدم وجود آليات متابعة فعّالة.

**أهداف البحث**

1. دراسة القوانين العراقية المتعلقة بالأمن السيبراني.
2. مقارنة هذه القوانين بالمعايير الدولية.
3. تحديد نقاط القوة والضعف في الالتزام بهذه المعايير.
4. تقديم توصيات لتعزيز تطبيق المعايير على المستوى الوطني.

المنهجية:

- المنهج الوصفي التحليلي لدراسة القوانين والاتفاقيات الدولية.
- المنهج المقارن لمقارنة التشريعات العراقية بالمعايير الدولية.
- منهج دراسة الحالة لتحليل التجارب والحوادث العملية في العراق

**المبحث الأول**

**الإطار القانوني والتنظيمي للأمن السيبراني في العراق**

**لمحة عامة عن التشريعات العراقية في مجال الأمن السيبراني وأهميتها**

أدّى التطور التكنولوجي المتسارع واعتماد الدولة العراقية المتزايد على الأنظمة الرقمية في إدارة شؤونها الإدارية والمالية والخدمية إلى بروز نوع جديد من المخاطر، تمثّل بالتهديدات السيبرانية التي تستهدف المعلومات والأنظمة الإلكترونية ولم تعد هذه التهديدات مقتصرة على الأفراد، بل امتد أثرها ليشمل مؤسسات الدولة، والبنى التحتية الحيوية، والقطاع المصرفي، والاتصالات، الأمر الذي جعل مسألة الأمن السيبراني من القضايا الجوهرية المرتبطة بالأمن الوطني.

وفي ظل هذا الواقع، برزت الحاجة إلى وجود إطار قانوني ينظم استخدام الفضاء السيبراني، ويحدّد الأفعال غير المشروعة التي تُرتكب عبر الوسائل الإلكترونية، ويوفّر الحماية القانونية للمعلومات والأنظمة الرقمية وقد استجابت الدولة العراقية لهذه الحاجة من خلال سن مجموعة من التشريعات، كان في مقدمتها قانون جرائم المعلوماتية رقم 56 لسنة 2017، الذي مثّل خطوة تشريعية مهمة لمواكبة التطورات التقنية والحد من الجرائم المستحدثة التي لم تكن معروفة عند صدور القوانين التقليدية.

**المطلب الأول: التشريعات الوطنية المتعلقة بالأمن السيبراني**

**الفرع الأول: قانون جرائم المعلوماتية رقم 56 لسنة 2017**

جاء قانون جرائم المعلوماتية رقم 56 لسنة 2017 في سياق تشريعي اتسم بمحاولة سد الفراغ القانوني القائم في مواجهة الجرائم الإلكترونية، إذ إن قانون العقوبات العراقي رقم 111 لسنة 1969 وُضع لمعالجة الجرائم التقليدية، ولم يكن قادرًا على استيعاب طبيعة الجرائم الرقمية التي تتميز بالسرعة، وعدم التقيد بالمكان، وصعوبة تعقب الجناة.

ويهدف هذا القانون إلى وضع قواعد قانونية واضحة لمكافحة الجرائم المرتكبة باستخدام الحاسوب أو شبكة الإنترنت أو أي وسيلة تقنية أخرى، من خلال تجريم أفعال محددة تمس سرية

المعلومات وسلامتها وتوافرها، وهي العناصر الأساسية للأمن السيبراني [1]

وقد ركّز المشرّع العراقي في هذا القانون على حماية الأنظمة المعلوماتية من أي اختراق غير مشروع، سواء ترتب على ذلك ضرر فعلي أم لا، إذ اعتبر مجرد الدخول غير المصرح به إلى النظام المعلوماتي سلوكًا مجرّمًا، لما ينطوي عليه من تهديد محتمل لأمن المعلومات [2]، ويعكس هذا التوجه وعيًا بأهمية الوقاية المسبقة، وعدم الاكتفاء بمعالجة النتائج بعد وقوع الضرر.

ومن الجوانب المهمة التي عالجها القانون مسألة الاحتيال الإلكتروني والابتزاز الرقمي، إذ أصبحت هذه الجرائم من أكثر الجرائم شيوعًا في المجتمع العراقي، مستفيدة من ضعف الوعي التقني لدى بعض المستخدمين وقد سعى القانون إلى توفير حماية قانونية للأفراد من خلال تجريم كل سلوك يستغل الوسائل الإلكترونية لتهديد الضحية أو إجبارها على تقديم منفعة مالية أو معلومات شخصية [3]، كما تناول القانون تجريم الأفعال التي تؤدي إلى سرقة البيانات أو تعديلها أو إتلافها، لما لهذه الأفعال من آثار خطيرة على عمل المؤسسات العامة والخاصة، خصوصًا عندما تتعلق البيانات بأنظمة مصرفية أو سجلات حكومية أو معلومات شخصية للمواطنين ويُلاحظ أن المشرّع شدّد العقوبات في حال ارتكبت هذه الجرائم بقصد تحقيق منفعة مادية أو الإضرار بالمصلحة العامة [4].

وفي إطار تعزيز فعالية المنظومة القضائية، نظم قانون جرائم المعلوماتية مسألة التعامل مع الأدلة الرقمية، من خلال إقرار حجيتها متى ما تم جمعها وفق الإجراءات القانونية، وهو ما يُعد تطورًا مهمًا في النظام القضائي العراقي، نظرًا لأن الإثبات في الجرائم السيبرانية يعتمد بدرجة كبيرة على الوسائل التقنية [1].

ورغم أهمية هذا القانون، إلا أن تطبيقه العملي واجه عدة تحديات، أبرزها غموض بعض المصطلحات القانونية المستخدمة فيه، مثل مفهوم "النظام المعلوماتي "المحتوى المخالف"، الأمر الذي يفتح المجال لاختلاف التفسير القضائي، وقد يؤدي إلى تباين الأحكام [3].

كما يُؤخذ على القانون عدم وضع ضوابط دقيقة تضمن التوازن بين متطلبات الأمن السيبراني وحماية الحقوق والحريات الأساسية، ولا سيما حرية التعبير والحق في الخصوصية، وهو ما أثار جدلًا فقهيًا حول مدى انسجام بعض نصوصه مع المعايير الدولية لحقوق الإنسان [4].

إلى جانب ذلك، فإن ضعف الكوادر المتخصصة في مجال التحقيق الرقمي، وقلة الخبرة التقنية لدى بعض الجهات المختصة، يمثلان عائقًا حقيقيًا أمام التطبيق الفعلي لنصوص القانون، إذ إن الجرائم السيبرانية تتطلب مهارات فنية عالية وأدوات تقنية متقدمة [5]

وبناءً على ما تقدم، يمكن القول إن قانون جرائم المعلوماتية رقم 56 لسنة 2017 يُعد حجر الأساس في الإطار القانوني للأمن السيبراني في العراق، إلا أن فعاليته تظل مرهونة بتطوير النصوص القانونية، وبناء القدرات البشرية، وتعزيز البنية المؤسسية، بما ينسجم مع المعايير الدولية للأمن السيبراني.

**الفرع الثاني: القوانين المكملة للأمن السيبراني**

**أولًا: أهمية القوانين المكملة في الأمن السيبراني**

بالرغم من أن قانون جرائم المعلوماتية رقم 56 لسنة 2017 هو التشريع الرئيسي لمكافحة الجرائم الإلكترونية في العراق، إلا أن إعماله وحده لا يكفي لضمان حماية شاملة في المجال السيبراني وذلك لأن الأمن السيبراني ليس قضية تشريعية معزولة، بل يمتد تأثيرها إلى نصوص قانونية أخرى تتداخل مع حماية البيانات، الجرائم التقليدية ذات البعد الرقمي، وإجراءات العمل الحكومي الرقمي.

ومن هنا، ظهرت الحاجة إلى وجود قوانين مكملة تُعالج الجوانب التي لا يغطيها قانون جرائم المعلوماتية بشكل مباشر، أو تعمل على دعم تطبيقه، مثل قانون العقوبات العراقي، قوانين حماية البيانات، والتعليمات الوزارية التي تصدرها الجهات التنفيذية لتنظيم العمل الرقمي داخل مؤسسات الدولة.

ثانيًا: قانون العقوبات العراقي رقم 111 لسنة 1969 ودوره في الأمن السيبراني

على الرغم من أن قانون العقوبات رقم 111 لسنة 1969 وُضع قبل أن يصبح الفضاء الرقمي جزءًا أصيلًا من الحياة العامة، إلا أنه ما يزال يعمل كقانون تكميلي لمعالجة بعض الجرائم الرقمية التي ربما لا يغطيها قانون جرائم المعلوماتية بشكل مباشر، وبخاصة في الحالات التي تتصل بجرائم تقليدية تتخذ صيغًا إلكترونية.

فعلى سبيل المثال، يمكن الاستناد إلى نصوص القانون في الجرائم التي تتعلق بالاعتداء على الأموال أو السرقات إذا ارتبطت بالسلوك الرقمي بطريقة تؤدي إلى إلحاق الضرر بمصالح الآخرين، إذ ينص القانون على عقوبات السطو والسرقة والاحتيال بشكل عام، وهذا يشمل الحالة التي يتم فيها ارتكاب الجريمة باستخدام الوسائل الإلكترونية ما لم يتم تفرّد القانون المعلوماتي بها [5].

كما أن بعض الجرائم التقليدية مثل التزوير قد تتخذ شكلًا رقميًا في حال تم تزوير مستندات إلكترونية أو بيانات محفوظة على أنظمة رقمية، وبالتالي يُعاد تطبيق نصوص قانون العقوبات على تلك الأفعال لتغطية ثغرات تشريعية قد تظهر أثناء المقاضاة [6].

**ثالثًا: قوانين حماية لبيانات والخصوصية**

مع التطور الرقمي وانتشار التعاملات الإلكترونية، ظهرت الحاجة إلى حماية بيانات الأفراد من الاستخدام غير المصرح به أو التسريب أو البيع، خصوصًا بعد أن أصبحت البيانات الشخصية تُجمع وتُخزن في قواعد بيانات إلكترونية ضمن المؤسسات الحكومية والخاصة.

في العراق، لا يوجد قانون منفصل وشامل لحماية البيانات الشخصية كما هو الحال في بعض الدول المتقدمة، لكن هناك محاولات تشريعية وتنظيمية لاحتواء هذه الحاجة، منها مواد منتشرة في قوانين مختلفة تضبط حماية المعلومات الخاصة بالأفراد، مثل قانون الخدمة المدنية واتفاقيات سرية الوظيفة التي تفرض على الموظف حظر الكشف عن بيانات المواطنين التي يطلع عليها بحكم العمل [2].

كما أن بعض الجهات الحكومية أصدرت تعليمات لحماية البيانات الخاصة بالمراجعين والمستفيدين داخل دوائرها، بهدف ضمان سرية المعلومات ومنع استخدامها أو تداولها بدون موافقة قانونية، ما يعكس وعيًا متزايدًا بأهمية حماية الخصوصية في الفضاء الرقمي [1].

**رابعًا: التعليمات الوزارية والتنظيمات الداخلية**

تلعب التعليمات الوزارية والتنظيمات الداخلية دورًا مهمًا في دعم تنفيذ القوانين المتعلقة بالأمن السيبراني، لأنها تمكّن الجهات الحكومية من تنظيم إجراءات العمل الرقمي داخل دوائرها، وتحديد السياسات الأمنية، والمسؤوليات التقنية، وآليات التحقيق الداخلي في حال وقوع خروقات.

فعلى سبيل المثال، أصدرت بعض الوزارات، مثل وزارة الداخلية ووزارة الاتصالات، تعليمات تنظيمية تتضمن قواعد لتأمين الأنظمة المعلوماتية، وإجراءات للتعامل مع الحوادث الرقمية، وتحديد آليات الصيانة الدورية للبنية التحتية التكنولوجية، وإجراءات التحقيق في الحوادث السيبرانية بالتعاون مع الجهات القضائية المختصة [3].

وتأتي هذه التعليمات كإضافات تنفيذية تساهم في ترجمة النصوص القانونية إلى إجراءات عملية يمكن تطبيقها داخل المؤسسات، مما يعالج جزءًا من النقص في التطبيق العملي للقوانين الرسمية عند وقوع الحوادث الرقمية.

**خامسًا: التحديات المتعلقة بالقوانين المكملة**

رغم أهمية هذه القوانين المكملة والتنظيمات الداخلية، إلا أن هناك مجموعة من التحديات التي تؤثر على فاعليتها:

1. عدم وجود قانون شامل لحماية البيانات الشخصية بشكل مستقل، ما يحد من قدرة العراق على حماية خصوصية المواطنين في الفضاء الرقمي [7].
2. تعارض أو ازدواجية بين نصوص قانون العقوبات وقانون جرائم المعلوماتية في بعض الحالات، ما يخلق صعوبة في الاختيار بين القانونين أثناء الإجراء القضائي [5].
3. ضعف التحديث المستمر للتعليمات الوزارية، إذ تظل بعضها غير مواكبة للتطورات السريعة في تقنية المعلومات، مما يقلل من فعاليتها في مواجهة الهجمات والتحديات الحديثة [2].
4. نقص التدريب المؤسسي في دوائر الدولة على كيفية تطبيق هذه التعليمات القانونية والتنظيمية، ما يجعل بعضها حجريًا وغير قابل للتطبيق الفعلي [4].

**الفرع الثالث: الهيئات الوطنية المختصة بالأمن السيبراني في العراق**

**أولًا: أهمية الهيئات الوطنية في الأمن السيبراني**

إن سن التشريعات القانونية للأمن السيبراني لا يضمن وحده حماية المعلومات والأنظمة الرقمية، إذ يلزم وجود هيئات وطنية متخصصة تكون مسؤولة عن تطبيق القوانين ومراقبة الالتزام بها، وتطوير السياسات والإجراءات التي تعزز من الأمن السيبراني اذ ان هذه الهيئات تمثل الجهة التنفيذية والرقابية الفعلية التي تتحمل مسؤولية حماية البنى التحتية الرقمية، متابعة الهجمات الإلكترونية، وتنفيذ التعليمات الوزارية والقوانين ذات الصلة.

في العراق، برزت عدة هيئات وطنية تلعب دورًا مركزيًا في هذا المجال، من أبرزها: وزارة الاتصالات، جهاز الأمن الوطني، ومراكز الرقابة التقنية داخل الوزارات والدوائر الحكومية.

ثانيًا: وزارة الاتصالات العراقية ودورها في الأمن السيبراني

تلعب وزارة الاتصالات دورًا محوريًا في إدارة البنية التحتية الرقمية وحماية الشبكات الوطنية، إذ تتولى الوزارة مسؤولية تأمين خطوط الاتصال، مراكز البيانات، وأنظمة الإنترنت التي تعتمد عليها المؤسسات الحكومية والخاصة.

وتقوم الوزارة بعدة مهام تتعلق بالأمن السيبراني، منها:

1. تطوير السياسات الوطنية للأمن السيبراني بما يتوافق مع التشريعات المحلية والمعايير الدولية.
2. إصدار التعليمات التقنية واللوائح الداخلية للدوائر الحكومية لضمان حماية البيانات والمعلومات الرقمية.
3. التنسيق مع الجهات الأمنية والقضائية عند وقوع أي اختراق أو تهديد سيبراني [1].

ويلاحظ الباحثون أن دور وزارة الاتصالات أصبح أكبر مع تزايد اعتماد الحكومة الإلكترونية والخدمات الرقمية على شبكة الإنترنت، خصوصًا في مجالات مثل البنوك، الصحة، والطاقة، حيث أصبح تأمين هذه الشبكات أمرًا حيويًا لاستقرار الدولة [3].

**ثالثًا: جهاز الأمن الوطني ودوره الرقابي والتنفيذي**

يعد جهاز الأمن الوطني من أهم الجهات المختصة في العراق لمكافحة الجرائم الإلكترونية، إذ يضطلع بمسؤوليات المراقبة الأمنية، التحقيق في الهجمات السيبرانية، والتعاون مع الجهات القضائية لتطبيق القانون رقم 56 لسنة 2017.

ومن مهامه الأساسية:

- متابعة أي نشاط مشبوه على الشبكات الحكومية والخاصة التي تؤثر على الأمن الوطني.
- تقديم الدعم الفني والتقني للجهات الحكومية عند وقوع هجمات سيبرانية.
- التنسيق مع وزارة الاتصالات لضمان تأمين البنية التحتية الرقمية وحماية البيانات الحساسة [2]

ويؤكد الخبراء العراقيون أن دور الجهاز لا يقتصر على المراقبة الأمنية التقليدية، بل يشمل تطوير القدرات الفنية للكشف المبكر عن الهجمات، وهذا يعزز من فعالية القانون ويحد من الخسائر الناتجة عن الجرائم الرقمية [8].

**رابعًا: مراكز الرقابة التقنية في المؤسسات الحكومية**

تمثل مراكز الرقابة التقنية في الوزارات والدوائر الحكومية أدوات تنفيذية حيوية لمتابعة تطبيق القانون وضمان حماية المعلومات، إذ تقوم بالمهام التالية:

1. رصد الأنشطة الرقمية واكتشاف أي اختراق أو محاولة وصول غير مصرح بها.
2. تطبيق الإجراءات التقنية الوقائية، مثل أنظمة الجدار الناري (Firewall) وبرامج مكافحة الفيروسات وحماية قواعد البيانات.
3. تقديم تقارير دورية لوزارة الاتصالات وجهاز الأمن الوطني عن مستوى الالتزام بالقوانين والتعليمات الخاصة بالأمن السيبراني [4].

وتعد هذه المراكز الرابط الأساسي بين النص القانوني وتنفيذه عمليًا داخل المؤسسات، حيث تتحول القوانين المكتوبة إلى إجراءات يومية قابلة للتطبيق.

**خامسًا: التحديات التي تواجه الهيئات الوطنية**

رغم الدور المحوري لهذه الهيئات، إلا أنها تواجه عدة تحديات تحد من فعالية عملها:

1. نقص الكوادر الفنية المتخصصة في الأمن السيبراني داخل الوزارات والمراكز الحكومية.
2. قلة التنسيق بين الهيئات المختلفة، مما يؤدي أحيانًا إلى ازدواجية أو خلل في الإجراءات الأمنية.
3. ضعف التحديث المستمر للبنية التحتية التقنية، وهو ما يجعل بعض الشبكات عرضة للهجمات الحديثة.
4. عدم وجود موازنات كافية لتطوير المعدات والأنظمة الأمنية الرقمية في الوقت المناسب، ما يحد من قدرة المؤسسات على الاستجابة للطوارئ السيبرانية [6].

**المطلب الثاني**

**المعايير والإطار التنظيمي الدولي للأمن السيبراني**

**الفرع الأول: المعايير الدولية**

مع التوسع الكبير في استخدام التكنولوجيا الحديثة والاعتماد المتزايد على الشبكات الرقمية في جميع مجالات الحياة، أصبح الأمن السيبراني مسألة استراتيجية تمس الأمن الوطني والاقتصاد والخدمات الأساسية وفي هذا السياق، ظهرت الحاجة إلى وجود معايير دولية واضحة توجه الدول والمؤسسات نحو إدارة مخاطر المعلومات بشكل فعال، وتساعد على حماية البيانات الحساسة والتعامل مع التهديدات الإلكترونية المعقدة.

**أولًا: معيار ISO/IEC 27001 [7]**

يُعد ISO/IEC 27001 معيارًا عالميًا لإدارة أمن المعلومات، يحدد إطارًا منهجيًا لإدارة المخاطر السيبرانية بهدف حماية سرية البيانات وسلامتها وتوافرها ويستند المعيار إلى مجموعة من المبادئ الأساسية التي يجب على المؤسسات اتباعها:

1. تقييم المخاطر وتحديد الثغرات: يتطلب المعيار تحليل جميع الأصول الرقمية، تحديد نقاط الضعف والتهديدات المحتملة، وتقدير تأثيرها على سير العمل وهذا يتيح وضع خطط حماية دقيقة ومبنية على أدلة علمية

2. وضع سياسات وإجراءات أمنية: يفرض ISO/IEC 27001 إنشاء سياسات واضحة لإدارة البيانات، تشمل ضوابط الوصول، وإجراءات التعامل مع المعلومات الحساسة، ومسؤوليات كل موظف، مما يضمن وجود إطار قانوني وتنظيمي داخلي لتطبيق الحماية.

3. التحكم في الوصول والمصادقة: يركز المعيار على منع الوصول غير المصرح به للأنظمة والمعلومات، بما يشمل إدارة كلمات المرور، تصاريح الدخول، والمصادقة متعددة العوامل، لضمان أن الوصول إلى المعلومات محصور فقط بالمخولين.
4. استمرارية الأعمال والتعافي من الكوارث: يضع المعيار آليات لضمان استمرار عمل المؤسسة في حال وقوع أي حادثة سيبرانية، من خلال خطط التعافي واستعادة البيانات، ما يقلل من تأثير الهجمات على العمليات الحيوية [8].

يعد هذا المعيار أداة أساسية للمؤسسات التي تسعى إلى التحول الرقمي الآمن، حيث يضمن ليس فقط حماية البيانات، بل أيضًا تعزيز ثقة العملاء والشركاء الدوليين في قدرة المؤسسة على التعامل مع التهديدات الحديثة.

**ثانيًا: إطار NIST للأمن السيبراني**

أصدر المعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة إطارًا مرنًا لإدارة الأمن السيبراني، يعرف بـ NIST Cybersecurity Framework. يعتمد هذا الإطار على خمسة محاور رئيسية: [7]

1. التعرف (Identify): يتضمن فهم البيئة الرقمية للمؤسسة، تحديد الأصول الحيوية، وتصنيف المخاطر المحتملة وهذه المرحلة أساسية لتحديد الأولويات ووضع الخطط الوقائية.
2. الحماية (Protect): تطبيق التدابير الوقائية مثل تشفير البيانات، أنظمة مراقبة الشبكات، وضوابط الوصول والهدف هو الحد من احتمالية حدوث اختراقات.
3. الكشف (Detect): إنشاء أنظمة للكشف المبكر عن أي نشاط غير طبيعي أو محاولات اختراق، مما يتيح الاستجابة الفورية قبل أن تتفاقم المشكلة.
4. الاستجابة (Respond): وضع خطط للتعامل مع الحوادث عند حدوثها، بما يشمل تنسيق الفرق الفنية والإدارية، وإبلاغ الجهات المعنية.
5. التعافي (Recover): استعادة العمليات والأنظمة المتأثرة بسرعة لضمان استمرار العمل دون خسائر كبيرة، مع تحسين الإجراءات لمنع تكرار الحوادث.

يمتاز إطار NIST بالمرونة، إذ يمكن تطبيقه على جميع أنواع المؤسسات، سواء كانت حكومية أو خاصة، ويتيح دمج الإجراءات مع المعايير الأخرى مثل ISO/IEC 27001، ما يخلق إطارًا شاملًا وقابلًا للتطوير وفق الاحتياجات المؤسسية والدولية [8].

**ثالثًا: أهمية اعتماد هذه المعايير دوليًا**

تطبيق هذه المعايير الدولية يوفر مزايا استراتيجية كبيرة:

- توحيد الإجراءات والممارسات الأمنية بين الدول والمؤسسات، ما يسهل التعاون الدولي ومكافحة الجرائم السيبرانية العابرة للحدود.
- تقليل المخاطر المحتملة من خلال تقييم دقيق للتهديدات واتخاذ الإجراءات الوقائية قبل حدوث الضرر.
- تعزيز الثقة والمصداقية أمام العملاء والشركاء الدوليين، خصوصًا في مجالات مثل البنوك والخدمات الحكومية والخاصة.
- تحقيق الاستمرارية المؤسسية، إذ توفر هذه المعايير آليات واضحة للتعامل مع الهجمات والتعافي من الأضرار بسرعة وكفاءة، مما يقلل من الخسائر الاقتصادية والمعنوية [9].

اعتماد هذه المعايير ليس مجرد إجراء تقني، بل يمثل سياسة استراتيجية وطنية، إذ يضمن أن المؤسسات العراقية قادرة على حماية بياناتها والبنية التحتية الرقمية وفق أفضل الممارسات العالمية، ويهيئها للتعاون الدولي ومواكبة التطورات في الأمن السيبراني.

**الفرع الثاني: التزامات العراق تجاه الاتفاقيات الدولية**

**أولًا: السياق الدولي للأمن السيبراني**

مع اتساع الاعتماد على الفضاء الرقمي في الخدمات الحكومية والبنى التحتية الحيوية، أخذ الأمن السيبراني بعدًا دوليًا مشتركًا لأن الهجمات السيبرانية لا تعترف بالحدود الجغرافية، فقد بات من الضروري أن تتعاون الدول فيما بينها عبر اتفاقيات متعددة تهدف إلى تبادل الخبرات، تنسيق الاستجابة للتهديدات، وتوحيد المعايير الفنية والقانونية.

من هنا ظهرت الاتفاقيات الدولية التي تضم مؤسسات دولية مثل الاتحاد الدولي للاتصالات (ITU)، الذي يعد جهازًا متخصصًا للأمم المتحدة، ويهتم بتنظيم شبكات الاتصالات والمعلومات، وتقديم الدعم الفني للدول الأعضاء في مجال الأمن السيبراني [8].

**ثانيًا: عضوية العراق في إطار الاتحاد الدولي للاتصالات والتزاماتها**

العراق عضــو في الاتحاد الدولي للاتصالات منذ عقود، ويشارك في مؤتمراته واجتماعاته الفنية وبموجب انخراط العراق في هذا الإطار الدولي، يلتزم بعدد من المبادئ الأساسية المتعلقة بالأمن السيبراني، منها:

1. تطوير سياسات واستراتيجيات وطنية تتماشى مع المعايير الفنية التي يصدرها الاتحاد الدولي للاتصالات لتعزيز حماية شبكات الاتصالات والبنى التحتية الرقمية.
2. مشاركة المعلومات التقنية والتقارير الخاصة بالتهديدات السيبرانية من خلال القنوات الدولية، ما يساهم في تعزيز القدرة على توقع الأخطار والاستجابة لها بشكل أسرع.
3. الالتزام بتوصيات الحلول التقنية والتدابير الوقائية التي يقترحها الاتحاد، مثل تبني أساليب التشفير القوية، والحفاظ على استمرارية خدمات الاتصالات، وتعزيز قدرات الاستجابة للحوادث الأمنية [9].

هذه الالتزامات تؤكد أن العراق ليس معزلًا في مواجهة التحديات الرقمية، بل هو جزء من منظومة دولية تسعى إلى رفع مستوى الأمن السيبراني عالميًا.

**ثالثًا: التزامات العراق تجاه اتفاقيات أخرى ذات صلة**

بالإضافة إلى الاتحاد الدولي للاتصالات، هناك عدد من الاتفاقيات والمبادرات الدولية التي يرتبط العراق بها بصورة مباشرة أو غير مباشرة في مجال الأمن السيبراني:

- اتفاقيات الأمم المتحدة لمكافحة الجرائم السيبرانية: هذه الاتفاقيات تدعو الدول الأعضاء إلى التعاون في التحقيقات والتحقيقات المشتركة في الجرائم المعلوماتية العابرة للحدود، وتبادل الأدلة والخبرات التقنية، وهو ما يعزز فعالية القوانين المحلية مثل قانون رقم 56 لسنة 2017.
- المبادرات الإقليمية للتعاون الأمني الرقمي: بعض الدول الأعضاء في الجامعة العربية تشارك في منتديات ومبادرات لتنسيق الجهود في مواجهة الهجمات الرقمية، ما يشكل إطارًا إضافيًا للعراق للاستفادة من الخبرات الإقليمية والإقليمية في هذا المجال.

الالتزام بهذه الاتفاقيات لا يعني فقط توقيع نصوص، بل يستلزم ترجمة هذه الالتزامات إلى سياسات وإجراءات عملية في القوانين الوطنية، والهيئات المختصة، والأنظمة التقنية، وهو ما يتطلب تحديثات مستمرة في التشريعات والبنى التحتية.

**رابعًا: التحديات التي تواجه العراق في تنفيذ التزاماته الدولية**

رغم انخراط العراق في هذه الاتفاقيات، ثمة تحديات عملية تعيق التنفيذ الكامل:

1. ضعف البنية التحتية التقنية في بعض المؤسسات الحكومية يعوق تطبيق التوصيات الفنية الصادرة عن الاتحاد الدولي للاتصالات.
2. نقص الخبرات الفنية المتخصصة في مجال الأمن السيبراني، ما يجعل تنفيذ التزامات التبادل التقني والتعاون الدولي محدودًا.
3. عدم وجود استراتيجية وطنية متكاملة محدثة للأمن السيبراني تربط بين المتطلبات الدولية والتنفيذ المحلي، ما يؤدي إلى فجوات في الالتزام الفعلي [10].

رغم هذه التحديات، فإن وجود التزامات دولية يُشكل إطار ضغط إيجابي يدفع إلى تطوير التشريعات، بناء القدرات، وتعزيز التعاون الدولي، ما يسهم في بناء منظومة وطنية أكثر قوة لحماية الأمن السيبراني.

**الفرع الثالث: مقارنة أولية بين التشريعات الوطنية والمعايير الدولية**

**أولًا: السياق العام للمقارنة**

تسعى الدول إلى حماية بنيتها الرقمية ومعلوماتها الحساسة من الهجمات الإلكترونية عبر إصدار قوانين محلية صارمة وتبني المعايير الدولية للأمن السيبراني. في حالة العراق، تم وضع عدة تشريعات وطنية، أبرزها:

- قانون جرائم المعلوماتية رقم 56 لسنة 2017.
- قانون العقوبات العراقي الذي يعاقب الجرائم الرقمية.
- التعليمات الوزارية واللوائح التنظيمية الخاصة بحماية البيانات والمعلومات.

أما على المستوى الدولي، فتتضمن المعايير الأكثر اعتمادًا: [8] [7]

- ISO/IEC 27001: معيار إدارة أمن المعلومات.
- NIST Cybersecurity Framework: إطار لإدارة المخاطر السيبرانية.
- اتفاقيات الاتحاد الدولي للاتصالات وغيرها من الاتفاقيات الدولية المتعلقة بالجرائم الإلكترونية وحماية البيانات.

تهدف المقارنة الأولية إلى تحديد نقاط التوافق والفجوات بين التشريعات الوطنية والمعايير الدولية، بهدف تقييم مدى قدرة العراق على الالتزام بالمعايير العالمية للأمن السيبراني.

**ثانيًا: نقاط التوافق**

1. وجود قاعدة قانونية لتجريم الجرائم السيبرانية

يشمل قانون جرائم المعلوماتية رقم 56 لسنة 2017 نصوصًا واضحة لمعاقبة اختراق الأنظمة، سرقة البيانات، والجرائم الرقمية، ما يتوافق مع المتطلبات الدولية لحماية المعلومات [1].

2. وجود هيئات مختصة لمراقبة وتنفيذ القانون

مثل وزارة الاتصالات، جهاز الأمن الوطني، ومراكز الرقابة التقنية، وهذه الهيئات تتوافق مع توصيات المعايير الدولية بضرورة وجود جهة مسؤولة عن تطبيق السياسات الأمنية [11].

3. تعليمات تنظيمية داخلية

صدرت عدة تعليمات وزارية تنظم حماية البيانات وإجراءات الوصول، وهو ما يتوافق مع المتطلبات الأساسية في ISO/IEC 27001 وNIST فيما يتعلق بالسياسات الداخلية والتحكم في الوصول [8].

**ثالثًا: نقاط الاختلاف والفجوات**

1. ضعف البنية التحتية الرقمية

بعض المؤسسات الحكومية في العراق لا تمتلك أنظمة حديثة لمراقبة الشبكات بشكل فعال، ما يقلل من إمكانية تطبيق معايير NIST للكشف والاستجابة السريعة [7].

2. نقص الكوادر الفنية المتخصصة

ISO/IEC 27001 وNIST Framework يتطلبان خبرات فنية متقدمة، لكن المؤسسات العراقية تعاني من نقص الكوادر المدربة على التعامل مع التهديدات المعقدة.

3. غياب التشريعات الشاملة لحماية البيانات الشخصية

بينما تركز المعايير الدولية على حماية جميع أنواع البيانات الحساسة وتقييم المخاطر، التشريعات الوطنية العراقية محدودة نسبيًا في هذا المجال، مما يخلق فجوة في التوافق الكامل مع المعايير الدولية.

4. نقص التنسيق بين الهيئات الوطنية

المعايير الدولية تؤكد على وجود تنسيق متكامل بين جميع الجهات ذات العلاقة، لكن العراق يواجه تحديًا في دمج جهود وزارة الاتصالات، جهاز الأمن الوطني، ومراكز الرقابة التقنية بشكل فعال.

**رابعًا: ملاحظات تحليلية**

- يمكن القول إن العراق بدأ بخطوات مهمة نحو تنظيم الأمن السيبراني من خلال القوانين والهيئات الوطنية، ولكنه يحتاج إلى تطوير مستمر في البنية التحتية، الكوادر، والتشريعات لتحقيق الالتزام الكامل بالمعايير الدولية.
- اعتماد المعايير الدولية لا يعني فقط التوافق النظري، بل يتطلب تطبيقًا عمليًا على أرض الواقع يشمل تقييم المخاطر، حماية البيانات، والاستجابة للحوادث الرقمية.
- التوصيات المستقبلية تشمل: تحديث التشريعات الوطنية، تدريب الكوادر، تعزيز البنية التحتية، وتطوير سياسات متكاملة وفق المعايير الدولية.

**المبحث الثاني**

**مدى التزام العراق بالمعايير الدولية للأمن السيبراني**

مع تزايد الاعتماد على التكنولوجيا الحديثة في جميع القطاعات الحكومية والخاصة، أصبح الأمن السيبراني أحد الركائز الأساسية لحماية الدول والمؤسسات من التهديدات الرقمية والهجمات الإلكترونية ويعكس الالتزام بالمعايير الدولية للأمن السيبراني قدرة الدولة على حماية البنية التحتية الرقمية، المعلومات الحساسة، والبيانات الوطنية من الاختراق والتلاعب.

تأتي أهمية هذا الالتزام من كونه ليس مجرد التزام تقني، بل يمثل عنصرًا استراتيجيًا للأمن الوطني، حيث أن أي ضعف في حماية الشبكات والأنظمة قد يؤدي إلى توقف الخدمات الحيوية، تهديد الاقتصاد الوطني، أو تسرب معلومات حساسة إلى جهات غير مصرح لها.

في حالة العراق، على الرغم من وجود تشريعات وطنية، مثل قانون جرائم المعلوماتية رقم 56 لسنة 2017 والتعليمات الوزارية، إلا أن مدى مطابقة هذه القوانين للمعايير الدولية مثل ISO/IEC 27001، NIST Cybersecurity Framework، واتفاقيات الاتحاد الدولي للاتصالات يبقى محل تقييم وتحليل.

يهدف هذا المبحث إلى دراسة التزام العراق بهذه المعايير الدولية، من خلال تحليل التشريعات الوطنية، استعراض الالتزامات الدولية، ومقارنة الواقع المحلي مع المعايير العالمية، لتحديد نقاط القوة والضعف، والفجوات التي تحتاج إلى معالجة لضمان مستوى متقدم من الأمن السيبراني الوطني.

**المطلب الأول: التقييم العملي لتطبيق المعايير الدولية في العراق**

**الفرع الأول: تقييم البنية التحتية التقنية والتكنولوجية**

تُعد البنية التحتية التقنية والتكنولوجية الركيزة الأساسية لتطبيق المعايير الدولية للأمن السيبراني مثل ISO/IEC 27001 وNIST Cybersecurity Framework وفي العراق، يظهر التقييم العملي للبنية التحتية مزيجًا من الإنجازات والتحديات.

أولًا: الوضع الحالي للبنية التحتية التقنية

1. شبكات الاتصالات والإنترنت

تمتلك المؤسسات الحكومية خطوط اتصال أساسية، لكن ضعف التشفير وأنظمة الحماية الحديثة يجعلها عرضة للهجمات السيبرانية[12].

2. الخوادم وأنظمة التخزين

تعتمد المؤسسات على خوادم وأنظمة قديمة وغير متكاملة، ما يعيق تطبيق سياسات النسخ الاحتياطي والحماية من الكوارث، وهو مطلب أساسي في ISO/IEC 27001 [8].

3. أدوات الحماية والرقابة

كثير من المؤسسات تفتقر إلى جدران حماية متقدمة، أنظمة كشف التسلل، وبرامج إدارة المخاطر الرقمية، وهي عناصر رئيسية في تطبيق إطار NIST [7].

**ثانيًا: التحديات**

- نقص التمويل: عدم توفر ميزانيات كافية لتحديث الشبكات والبرامج الأمنية.
- قلة التكامل بين القطاعات: ضعف الربط بين الوزارات يجعل رصد التهديدات أقل فاعلية.
- نقص الكوادر الفنية: قلة الخبراء في الأمن السيبراني تؤثر على تطبيق المعايير الدولية.
- تعدد الجهات الرقابية: وزارة الاتصالات، جهاز الأمن الوطني، ومراكز الرقابة التقنية أحيانًا تعمل بشكل منفصل، مما يخلق ثغرات تطبيقية [1].

**ثالثًا: أهمية تطوير البنية التحتية**

- تأمين الشبكات والخوادم وفق ISO/IEC 27001.
- تطبيق أنظمة مراقبة واستجابة للحوادث الرقمية وفق NIST.
- تعزيز التكامل بين الجهات الحكومية والخاصة لتوحيد إدارة المخاطر السيبرانية.
- بناء قدرات بشرية متخصصة لإدارة البنية التحتية الرقمية بكفاءة [13].

تطوير هذه البنية يعزز قدرة العراق على الالتزام بالمعايير الدولية وحماية البنية التحتية الوطنية.

**الفرع الثاني: تدريب الكوادر وتأهيل الخبراء في مجال الأمن السيبراني**

تعتبر الموارد البشرية المؤهلة والمتخصصة أحد أهم عناصر نجاح تطبيق معايير الأمن السيبراني الدولية، مثل ISO/IEC 27001 وNIST Cybersecurity Framework" فالبنية التحتية الرقمية وحدها لا تكفي، بل يجب أن تكون هناك كوادر مدربة تستطيع إدارة المخاطر، مراقبة التهديدات، والاستجابة للحوادث السيبرانية بكفاءة.

**أولًا: الوضع الحالي لتدريب الكوادر في العراق**

1. وجود برامج تدريب محدودة

بعض الوزارات والمؤسسات العراقية توفر دورات قصيرة في الأمن الرقمي، لكنها غالبًا تركز على الجوانب النظرية فقط دون تغطية التطبيقات العملية والإطار الدولي للمعايير[10].

2. قلة الشهادات المهنية المعترف بها دوليًا

معظم الخبراء في العراق لا يحملون شهادات مثل CISSP أو CEH، وهي ضرورية لتطبيق المعايير الدولية بكفاءة [12].

3. ضعف الربط بين الجامعات والمؤسسات

هناك فجوة بين الجامعات التي تخرج مهندسين متخصصين وبين المؤسسات التي تحتاج إلى كوادر مؤهلة في الأمن السيبراني، مما يؤدي إلى نقص الخبراء المؤهلين عمليًا [11].

**ثانيًا: التحديات المرتبطة بتأهيل الخبراء**

- نقص التمويل لتوفير برامج تدريبية مكثفة ومستمرة.
- قلة الكوادر المتخصصة في تصميم وتنفيذ البرامج التدريبية المتقدمة.
- ضعف الثقافة السيبرانية في بعض المؤسسات، مما يقلل من جدية تطبيق التدريب.
- غياب الشراكات الدولية مع مراكز تدريب معترف بها، ما يعيق الاطلاع على أحدث التطورات والمعايير العالمية [1].

**ثالثًا: أهمية تطوير قدرات الكوادر البشرية**

- تدريب مستمر ومتخصص في جميع مستويات المؤسسة، من الفنيين إلى الإدارة العليا.
- منح شهادات معترف بها دوليًا لضمان الكفاءة في تطبيق المعايير الدولية.
- إنشاء مراكز تدريب وطنية مرتبطة بالجامعات والمؤسسات، لتغطية النقص في الخبرات.
- تشجيع التعاون الدولي مع مراكز الأبحاث والهيئات العالمية لتعزيز الخبرة العملية.

تطوير قدرات الكوادر البشرية يعزز قدرة العراق على تطبيق المعايير الدولية بفعالية، حماية البيانات الوطنية، واستجابة سريعة للهجمات السيبرانية.

**الفرع الثالث: حالات عملية وانتهاكات سيبرانية سابقة**

يعتبر تحليل الحوادث السيبرانية السابقة جزءًا مهمًا من تقييم مدى التزام العراق بالمعايير الدولية للأمن السيبراني، لأنه يعكس واقع

تطبيق السياسات والإجراءات الأمنية، ويظهر الثغرات التي تحتاج إلى معالجة.

**أولًا: أبرز الانتهاكات السيبرانية في العراق**

1. الهجمات على البنوك

شهد العراق عدة هجمات على الخدمات المصرفية الإلكترونية، مثل محاولات سرقة البيانات المالية للزبائن واختراق أنظمة الدفع الإلكتروني وهذه الهجمات كشفت ضعف البنية التحتية الأمنية وعدم كفاية الإجراءات الوقائية [13].

2. الهجمات على المؤسسات الحكومية

استهدفت هجمات إلكترونية بعض الوزارات والمصالح الحكومية، بما في ذلك محاولات تسريب البيانات الإدارية والمعلومات الحساسة وأظهرت هذه الحوادث نقص أنظمة كشف التسلل وأنظمة المراقبة المستمرة [14].

3. التصيد الإلكتروني والهجمات عبر البريد الإلكتروني

انتشرت محاولات التصيد والبرمجيات الخبيثة بين الموظفين الحكوميين، مما أدى إلى تسرب معلومات سرية وأثر على بعض الخدمات الإلكترونية[15].

**ثانيًا: تحليل الانتهاكات وأثرها على الالتزام بالمعايير الدولية**

- كشف الثغرات في البنية التحتية: الحوادث أظهرت نقاط ضعف في التشفير وإدارة البيانات، وهي متطلبات أساسية في ISO/IEC 27001.
- أهمية الكوادر البشرية: ضعف التدريب والتوعية أدى إلى استغلال الأخطاء البشرية في كثير من الانتهاكات، ما يؤكد الحاجة لتطوير الكوادر المؤهلة.
- ضرورة السياسات والإجراءات: معظم الهجمات كانت نتيجة غياب إجراءات موحدة لإدارة الحوادث والاستجابة للطوارئ، وهي متطلبات إطار NIST.

**ثالثًا: أهمية دراسة الحوادث العملية**

دراسة الانتهاكات السابقة تساعد على:

1. تحديد نقاط الضعف في المؤسسات قبل وقوع هجمات أكبر.
2. تحسين البنية التحتية والكوادر البشرية لتعزيز حماية المعلومات الوطنية.
3. تطبيق المعايير الدولية بشكل فعلي، وضمان الاستعداد لمواجهة الهجمات المستقبلية.
4. تطوير سياسات وقوانين لمواكبة التهديدات السيبرانية الحديثة [16].

**- ضعف التعاون الدولي والإقليمي في مجال تبادل المعلومات ومكافحة الجرائم الإلكترونية**

يُعد التعاون الدولي والإقليمي أحد الركائز المهمة لتعزيز الأمن السيبراني، إذ تعتمد الدول على تبادل المعلومات عن التهديدات، الاستفادة من الخبرات التقنية، والتنسيق لمكافحة الجرائم الإلكترونية العابرة للحدود.

**أولًا: الواقع الحالي للتعاون الدولي والإقليمي للعراق**

1. اتفاقيات محدودة

العراق عضو في بعض اتفاقيات الاتحاد الدولي للاتصالات (ITU)، لكنه لم يوقع أو يطبق العديد من البروتوكولات الدولية الأخرى المتعلقة بتبادل المعلومات السيبرانية [14].

2. ضعف التنسيق مع الجوار الإقليمي

هناك فجوة في التنسيق مع دول الجوار مثل الأردن والكويت وإيران فيما يتعلق بمكافحة الجرائم الإلكترونية وتبادل المعلومات عن التهديدات، ما يجعل المؤسسات العراقية أكثر عرضة للهجمات العابرة للحدود[7].

3. قلة الشراكات مع مراكز أبحاث عالمية

قلة التعاون مع المراكز البحثية المتخصصة والدولية حدّت من قدرة العراق على الاطلاع على أحدث طرق الحماية والاستجابة للهجمات السيبرانية.

**ثانيًا: أثر ضعف التعاون على الالتزام بالمعايير الدولية**

- يجعل العراق أقل قدرة على الاستجابة السريعة للهجمات العابرة للحدود.
- يقلل من إمكانية تبادل الخبرات والتجارب العملية لتطوير البنية التحتية والكفاءات البشرية.
- يضعف فرص العراق في الانضمام الكامل للمعايير والاتفاقيات الدولية المتعلقة بحماية البيانات والأمن الرقمي.

**ثالثًا: أهمية تعزيز التعاون الدولي والإقليمي**

- تبادل المعلومات والتهديدات السيبرانية مع الدول الأخرى لتقليل المخاطر.
- إبرام اتفاقيات تعاون وتقنيات مشتركة لمكافحة الجرائم الإلكترونية.
- الاستفادة من الخبرات الدولية لتطوير البنية التحتية والكفاءات البشرية.
- تعزيز دور العراق في المجالس والمنظمات الإقليمية والدولية الخاصة بالأمن السيبراني .

**خاتمة البحث**

خلصت الدراسة إلى أن العراق قد اتخذ خطوات أولية في وضع التشريعات المتعلقة بالأمن السيبراني، مثل قانون جرائم المعلوماتية رقم 56 لسنة 2017، لكن مدى الالتزام بالمعايير الدولية ما يزال محدودًا وتشير النتائج إلى أن العراق يواجه مجموعة من التحديات المرتبطة بالجانب التشريعي، التقني، البشري، والتمويلي، إضافة إلى ضعف التعاون الدولي والإقليمي، ما أثر على القدرة على حماية البنية التحتية الرقمية والمعلومات الحساسة.

**الاستنتاجات**

1. مراجعة وتحديث القوانين بما يتوافق مع المعايير الدولية، وإضافة آليات فعالة للرقابة والتطبيق العملي.
2. الاستثمار في البنية التحتية الرقمية من خلال تحديث الشبكات، الخوادم، وأنظمة الحماية.
3. إنشاء برامج تدريبية متقدمة ومتواصلة للكوادر البشرية، وربطها بشهادات دولية معترف بها.
4. تخصيص موارد مالية ثابتة لدعم مشاريع الأمن السيبراني وضمان استمرارية تطوير البنية التحتية.
5. تعزيز الشراكات الدولية والإقليمية لتبادل المعلومات ومواجهة الجرائم الإلكترونية بشكل فعال.
6. تأسيس وحدة وطنية مركزية لمكافحة الهجمات السيبرانية وربطها بالمؤسسات الحكومية لضمان الاستجابة الفورية والفعالة.

**التوصيات**

1. مراجعة وتحديث القوانين بما يتوافق مع المعايير الدولية، وإضافة آليات فعالة للرقابة والتطبيق العملي.
2. الاستثمار في البنية التحتية الرقمية من خلال تحديث الشبكات، الخوادم، وأنظمة الحماية.
3. إنشاء برامج تدريبية متقدمة ومتواصلة للكوادر البشرية، وربطها بشهادات دولية معترف بها.
4. تخصيص موارد مالية ثابتة لدعم مشاريع الأمن السيبراني وضمان استمرارية تطوير البنية التحتية.
5. تعزيز الشراكات الدولية والإقليمية لتبادل المعلومات ومواجهة الجرائم الإلكترونية بشكل فعال.
6. تأسيس وحدة وطنية مركزية لمكافحة الهجمات السيبرانية وربطها بالمؤسسات الحكومية لضمان الاستجابة الفورية والفعالة.

**المصادر**

[1] النجيفي علاء محمد. "الإطار القانوني والأمني للأمن السيبراني في العراق وتطبيق المعايير الدولية"، مجلة البحوث القانونية العراقية؛ 2021؛ المجلد 5، العدد.(1)

[2] الماسي نورهان حميد. "تحليل دور الهيئات الوطنية في حماية المعلومات الرقمية في العراق"، مجلة كلية القانون – جامعة بغداد؛ 2022؛ المجلد 8، العدد.(2)

[3] الخطيب رشا ناظم. "تحديات تطبيق قانون جرائم المعلوماتية في العراق ودور جهاز الأمن الوطني"، مجلة الدراسات القانونية؛ 2021؛ المجلد 14، العدد.(1)

[4] الحمامي أحمد ستار. "الجرائم السيبرانية في التشريع العراقي: تحليل قانون جرائم المعلوماتية رقم 56 لسنة 2017"، مجلة القانون والإنسان؛ 2020؛ المجلد 10، العدد.(3)

[5] قدوري أحمد منذر. "تطوير الهيئات الوطنية لتعزيز الأمن السيبراني في العراق"، مجلة البحوث القانونية؛ 2021؛ المجلد 9، العدد.(3)

[6] الحلو رنا عبد. "دور وزارة الاتصالات العراقية في الأمن السيبراني: تحليل السياسات والإجراءات"، مجلة العلوم القانونية العراقية؛ 2021؛ المجلد 7، العدد.(2)

[7] المعهد الوطني للمعايير والتقنية" .(NIST) إطار تحسين الأمن السيبراني للبنية التحتية الحيوية"، وزارة التجارة الأمريكية؛ 2018.

[8] منظمة التقييس الدولية" .(ISO/IEC) نظم إدارة أمن المعلومات ـــ المتطلبات"، جنيف؛ 2013. وينظر ايضاً:
الاتحاد الدولي للاتصالات" .(ITU) الرقم القياسي العالمي للأمن السيبراني لعام 2018"، جنيف؛ 2019.

[9] حسين علي حسين. "الأمن السيبراني: نظريات وتطبيقات"، بغداد، العراق: دار المدى العلمية؛ 2022.

[10] الشمري سامي سعد. "أهمية الكوادر البشرية في تعزيز الأمن الرقمي في المؤسسات"، مجلة الإدارة والقانون؛ 2020؛ المجلد 11، العدد.(3)

[11] الزهراني إبراهيم عبد الله أحمد. "التحديات في تأهيل الخبراء الأمنيين وتطبيق المعايير الدولية"، مجلة البحوث القانونية العراقية؛ 2021؛ المجلد 5، العدد.(1)

[12] الدهام رعد حسين. "ضعف التعاون الدولي والإقليمي وتأثيره على الأمن السيبراني في العراق"، مجلة البحوث القانونية العراقية؛ 2020؛ المجلد 4، العدد.(2)

[13] الطائي سيف محمد. "التنسيق الإقليمي بين دول الجوار لمكافحة الجرائم الإلكترونية: العراق نموذجًا"، مجلة العلوم القانونية العراقية؛ 2021؛ المجلد 7، العدد.(3)

[14] الكيلاني أحمد سامي. "التعاون الدولي في الأمن السيبراني: أسس وتطبيقات"، القاهرة، مصر: دار الفكر العربي؛ 2019.

[15] الموسوي علي محمود. "الأمن السيبراني والاتفاقيات الدولية: دراسة مقارنة"، بغداد، العراق: دار الحكمة للنشر؛ 2021.

[16] سالم محمد صالح. "مراكز الرقابة التقنية في المؤسسات الحكومية العراقية: الواقع والتحديات"، مجلة الإدارة العامة والقانون؛ 2022؛ المجلد 11، العدد.(4)