



لجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء  
للمؤسسات الأمنية في مدينة السليمانية

## الجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء للمؤسسات الأمنية في مدينة السليمانية

أ. م. عمر مصطفى محمد

جامعة السليمانية التقنية، معهد التقني  
دوكان، قسم الادارة الاعمال

م. م. صبريه كريم خالد

جامعة السليمانية التقنية، معهد التقني  
بكرجو، قسم الإدارة الالكترونية

البريد الإلكتروني Email : [sabria.khaland@spu.edu.iq](mailto:sabria.khaland@spu.edu.iq)

**الكلمات المفتاحية:** الإدارة الإلكترونية؛ الجرائم الإلكترونية؛ الأمن السيبراني؛ الابتزاز  
الإلكتروني؛ التحول الرقمي

### كيفية اقتباس البحث

خالد، صبريه كريم، عمر مصطفى محمد، الجرائم الإلكترونية والسيطرة عليها من خلال الإدارة  
الإلكترونية الفعالة. دراسة ميدانية حول آراء للمؤسسات الأمنية في مدينة السليمانية، مجلة مركز  
بابل للدراسات الانسانية، نيسان ٢٠٢٦، المجلد: ١٦، العدد: ٤ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف  
والنشر ( Creative Commons Attribution ) تتيح فقط للآخرين تحميل البحث  
ومشاركته مع الآخرين بشرط نسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو  
استخدامه لأغراض تجارية.

Registered في مسجلة في  
**ROAD**

Indexed في مفهرسة في  
**IASJ**

لجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء  
للمؤسسات الأمنية في مدينة السليمانية



## Electronic crimes and their control through effective electronic management-A field study of the view's security agencies in the city of Sulaymaniyah

**Assistant Lecturer: Sabria  
Karim Khand**

Sulaimani Polytechnic University,  
Bakrjo Technical Institute, Department  
of Electronic Management

**Assistant Professor Omar  
Mustafa Mohammed**

Sulaimani Polytechnic University, Dukan  
Technical Institute, Department of  
Business Administration

**Keywords** : E-Administration 'Cybercrime 'Cybersecurity 'Cyber-  
Extortion 'Digital Transformation

### How To Cite This Article

Khand, : Sabria Karim, Omar Mustafa Mohammed, Electronic crimes and their control through effective electronic management-A field study of the view's security agencies in the city of Sulaymaniyah, Journal Of Babylon Center For Humanities Studies, April 2026, Volume:16, Issue 4.

This is an open access article under the CC BY-NC-ND license  
(<http://creativecommons.org/licenses/by-nc-nd/4.0/>)



[This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.](http://creativecommons.org/licenses/by-nc-nd/4.0/)

### Abstract:

This paper discusses how Electronic Administration (E-Administration) can help to curb and prevent cyber and technological crimes in the security institutions in Sulaymaniyah city. As the digital technologies and online services continue to spread at a high rate, cybercrimes including electronic frauds, hacking, and cyber-extortion have grown to a great extent, becoming a serious threat to the security of institutions and the safety of the population. Thus, the implementation of efficient electronic administrative systems and cybersecurity policies has become a necessity in fighting these threats.

The research was carried out in the form of a descriptive-analytical study and the main data collection method was the structured questionnaire. A random sample of 67 managers, officials, and employees who work in security institutions in Sulaymaniyah were given the questionnaire, and 57 valid responses were collected and analyzed. The data obtained were evaluated with the help of various statistical methods, such as



frequencies, percentages, means, standard deviations, Pearson correlation analysis, and simple linear regression to investigate the connections and impact of the study variables.

The findings showed that there are a considerable positive correlation and impact between electronic administration and reduction of cyber and technological crimes. Specifically, technological infrastructure, cybersecurity practices, and electronic operations management were identified to be important in enhancing institutional security and minimizing vulnerabilities that can culminate into cybercrimes. The paper ends by providing a number of recommendations on how to improve digital infrastructure, improve cybersecurity policies, offer continuous employee training, and enhance institutional awareness to be effective in combating cyber threats

### الملخص

تتناول هذه الورقة البحثية كيفية مساهمة الإدارة الإلكترونية في الحد من الجرائم الإلكترونية والتقنية ومنعها في المؤسسات الأمنية بمدينة السليمانية، فمع استمرار انتشار التقنيات الرقمية والخدمات الإلكترونية بوتيرة متسارعة، تزايدت الجرائم الإلكترونية، بما فيها الاحتيال الإلكتروني والاختراق والابتزاز الإلكتروني، بشكل كبير، لتشكل تهديدًا خطيرًا لأمن المؤسسات وسلامة السكان، ولذا، بات تطبيق أنظمة إدارية إلكترونية فعالة وسياسات أمن سيبراني ضرورة ملحة لمكافحة هذه التهديدات.

أجري البحث على شكل دراسة وصفية تحليلية، وكانت الاستبانة المنظمة هي الأداة الرئيسية لجمع البيانات. وُرعت الاستبانة على عينة عشوائية مكونة من ٦٧ مديرًا ومسؤولًا وموظفًا يعملون في المؤسسات الأمنية بمدينة السليمانية، وُجمعت ٥٧ استجابة صالحة وخضعت للتحليل، وقيمت البيانات المُجمعة باستخدام أساليب إحصائية متنوعة، كالتكرارات والنسب المئوية والمتوسطات والانحرافات المعيارية وتحليل ارتباط بيرسون والانحدار الخطي البسيط، وذلك لدراسة العلاقات بين متغيرات الدراسة وتأثيرها.

أظهرت النتائج وجود ارتباط إيجابي كبير وتأثير ملموس بين الإدارة الإلكترونية والحد من الجرائم الإلكترونية والتقنية، وعلى وجه التحديد، تبين أن البنية التحتية التقنية، وممارسات الأمن السيبراني، وإدارة العمليات الإلكترونية، عناصر أساسية في تعزيز الأمن المؤسسي وتقليل الثغرات التي قد تؤدي إلى جرائم إلكترونية. وتختتم الورقة البحثية بتقديم عدد من التوصيات حول كيفية تحسين البنية التحتية الرقمية، وتطوير سياسات الأمن السيبراني، وتوفير تدريب مستمر للموظفين، وتعزيز الوعي المؤسسي، وذلك لضمان فعالية مكافحة التهديدات السيبرانية.



## مقدمة

على مدى العقود القليلة الماضية، أحدثت تقنيات المعلومات والاتصالات سريعة التطور تغييراً جذرياً في كيفية إدارة المؤسسات لوظائفها الإدارية وتقديم خدماتها. وقد شهدت التقنيات الرقمية بروز الإدارة الإلكترونية التي تُمكن المؤسسات من أتمتة وظائفها الإدارية، ما يجعلها أكثر شفافية وكفاءة في تقديم الخدمات. وبرز التحول الرقمي كإحدى الاستراتيجيات الرئيسية للحكومات والمؤسسات حول العالم، والتي تهدف إلى تحديث أطرها الإدارية وتعزيز أداء مؤسساتها (دافنبورت ورونانكي، ٢٠١٨؛ ميرجل وآخرون، ٢٠١٩).

تُمكن الإدارة الإلكترونية المؤسسات من استخدام الأنظمة الرقمية وقواعد البيانات وتقنيات الاتصال لتحسين عملية صنع القرار، وتقليل الإجراءات البيروقراطية، وتبادل المعلومات بين الإدارات والمؤسسات. تُسهم هذه التقنيات في تطوير هياكل حوكمة أكثر كفاءة، ما يُتيح للمؤسسات تقديم خدماتها بسرعة ودقة أكبر (الشبول وآخرون، ٢٠١٤؛ جيل-غارسيا، وآخرون، ٢٠١٨). ومع ذلك، فقد أدى التوسع في استخدام التقنيات الرقمية إلى ظهور تهديدات جديدة لأمن المعلومات والتهديدات السيبرانية.

تُعد الجرائم السيبرانية والتقنية من أبرز قضايا الأمن العالمي، إلى جانب التحول الرقمي السريع. تُعرّف الجريمة السيبرانية بأنها أفعال إجرامية تُرتكب باستخدام أجهزة الحاسوب أو الأجهزة الرقمية أو شبكات الاتصالات بهدف الوصول غير المصرح به إلى أنظمة المعلومات، أو سرقة المعلومات الحساسة، أو إلحاق أضرار مالية وتشغيلية (وول، ٢٠١٧؛ هولت وآخرون، ٢٠١٨). وقد تطورت هذه الجرائم بشكل كبير مع نمو الإنترنت والمنصات الرقمية، فأصبحت أكثر تعقيداً وأصعب في التتبع.

أصبح تزايد وتيرة الهجمات الإلكترونية وتعقيدها مصدر قلق بالغ للحكومات والمنظمات. فالاختراقات، وهجمات التصيد الاحتيالي، ونشر البرمجيات الخبيثة، وسرقة الهوية، وبرامج الفدية، والاحتيال الإلكتروني، كلها تهديدات إلكترونية حديثة قد تتسبب بخسائر مالية فادحة وتعطيل العمل في المؤسسات (كشتري، ٢٠٢١؛ يار وستاينميتز، ٢٠١٩). وقد دفع هذا الأمر المنظمات إلى إيلاء مزيد من الاهتمام لتعزيز الأمن السيبراني ووضع استراتيجيات للحوكمة الرقمية لحماية أصولها المعلوماتية وبنيتها التحتية التقنية.

ولمواجهة هذه التحديات، وضعت معظم الحكومات والمنظمات الدولية أطراً قانونية وآليات مؤسسية لمكافحة الجرائم الإلكترونية وتعزيز ممارسات الأمن السيبراني. وتؤكد هذه البرامج على ضرورة دمج خطط الأمن السيبراني مع الحلول الإدارية والتقنية لتوفير حماية فعالة ضد





التحديات الإلكترونية (برينر، ٢٠١٠؛ وول، ٢٠١٧). وبالتالي، يُعدّ تطبيق أنظمة إدارة إلكترونية ناجحة مع أمن سيبراني فعال أمراً بالغ الأهمية في الحد من التهديدات الإلكترونية وتعزيز قدرة المؤسسات على الصمود في وجه الجرائم التقنية.

### المبحث الأول: منهجية البحث

#### ١. مشكلة البحث

على الرغم من التوسع المتزايد في استخدام التقنيات الرقمية والأنظمة الإدارية الإلكترونية في المؤسسات الحكومية والخاصة، لا تزال الجرائم الإلكترونية والتقنية تتزايد عالمياً. وقد أدى الانتشار السريع لاستخدام الإنترنت والخدمات الإلكترونية والمعاملات الرقمية إلى خلق فرص جديدة للمجرمين الإلكترونيين لاستغلال الثغرات الأمنية في أنظمة المعلومات وشبكات الاتصالات (. (Holt, Bossler and seigfreid-Spellar,2018;Kshetri,2021)

أصبحت الجرائم الإلكترونية تحدياً خطيراً للمؤسسات، نظراً لأن المهاجمين يطورون باستمرار أساليب متقدمة لتجاوز أنظمة الأمان واستغلال نقاط الضعف في البنى التحتية التقنية، تشمل التهديدات الإلكترونية الحديثة هجمات التصيد الاحتيالي، والإصابة بالبرمجيات الخبيثة، وهجمات برامج الفدية، والوصول غير المصرح به إلى البيانات الحساسة، مما قد يتسبب في خسائر مالية فادحة ويضر بسمعة المؤسسات. (Yar and Steinmetz,2019)

لا تزال العديد من المؤسسات تواجه تحديات عديدة تحد من قدرتها على مكافحة الجرائم الإلكترونية بفعالية. تشمل هذه التحديات ضعف البنية التحتية التقنية، وعدم كفاية سياسات الأمان السيبراني، ومحدودية وعي الموظفين بالتهديدات الإلكترونية، ونقص التكامل بين الأنظمة الإدارية واستراتيجيات الأمان الرقمي، أظهرت دراسات سابقة أن ضعف الوعي بالأمن السيبراني وضعف آليات الحوكمة الرقمية يزيدان من تعرض المؤسسات للهجمات السيبرانية. (Gil-Garcia et al.,2018;Kshetri,2011)

وفي سياق العراق وإقليم كردستان، أدى الاعتماد المتزايد على التقنيات الرقمية في المؤسسات الحكومية والأمنية إلى زيادة أهمية مسألة مكافحة الجرائم السيبرانية، فالمؤسسات الأمنية مسؤولة ليس فقط عن حماية البنى التحتية الرقمية، بل أيضاً عن التصدي للتهديدات السيبرانية وضمان أمن نظم المعلومات.

لذا، تتمثل المشكلة الرئيسية لهذه الدراسة في بحث ما إذا كان تطبيق أنظمة إدارة إلكترونية فعالة يُسهم في الحد من الجرائم السيبرانية والتقنية داخل المؤسسات الأمنية، وبناءً على ذلك، يسعى هذا البحث إلى دراسة العلاقة بين الإدارة الإلكترونية -المتتمثلة في البنية التحتية التقنية، والأمن



السيبراني، وإدارة العمليات الإلكترونية- والجرائم السيبرانية والتقنية في المؤسسات الأمنية بمدينة  
السليمانية.

## ٢. أسئلة البحث

يسعى البحث للإجابة عن الأسئلة الآتية:

١. ما مستوى تطبيق الإدارة الإلكترونية في المؤسسات الأمنية في مدينة السليمانية؟
٢. ما مدى تأثير الإدارة الإلكترونية في الحد من الجرائم الإلكترونية والتكنولوجية؟
٣. ما مستوى وعي وخبرة العاملين في المؤسسات الأمنية في مجال التكنولوجيا والأمن السيبراني؟
٤. ما أبرز التحديات التي تعيق تطبيق الإدارة الإلكترونية الفعالة في المؤسسات الأمنية؟

## ٣. أهداف البحث

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف، من أهمها:

١. التعرف على مفهوم الإدارة الإلكترونية وأهميتها في المؤسسات الأمنية.
٢. تحليل العلاقة بين الإدارة الإلكترونية والحد من الجرائم الإلكترونية.
٣. تحديد دور البنية التحتية التكنولوجية والأمن السيبراني في مواجهة الجرائم الرقمية.
٤. تقديم مجموعة من التوصيات التي تساعد المؤسسات الأمنية على تطوير أنظمتها الإدارية والتقنية للحد من الجرائم الإلكترونية.

## ٤. المنهج البحث

اعتمد الباحث على المنهج الوصفي التحليلي.

أداة البحث: استبيان وُرِّع على عينة البحث.

مجتمع البحث: منتسبي المؤسسات الأمنية في السليمانية.

## ٥. هيكل البحث

المبحث الأول: الإطار العام (المقدمة، المشكلات، الأهداف).

المبحث الثاني: الإطار النظري (مفهوم الجريمة الإلكترونية والإدارة الإلكترونية).

المبحث الثالث: الإطار الميداني (تحليل بيانات الاستبيان).

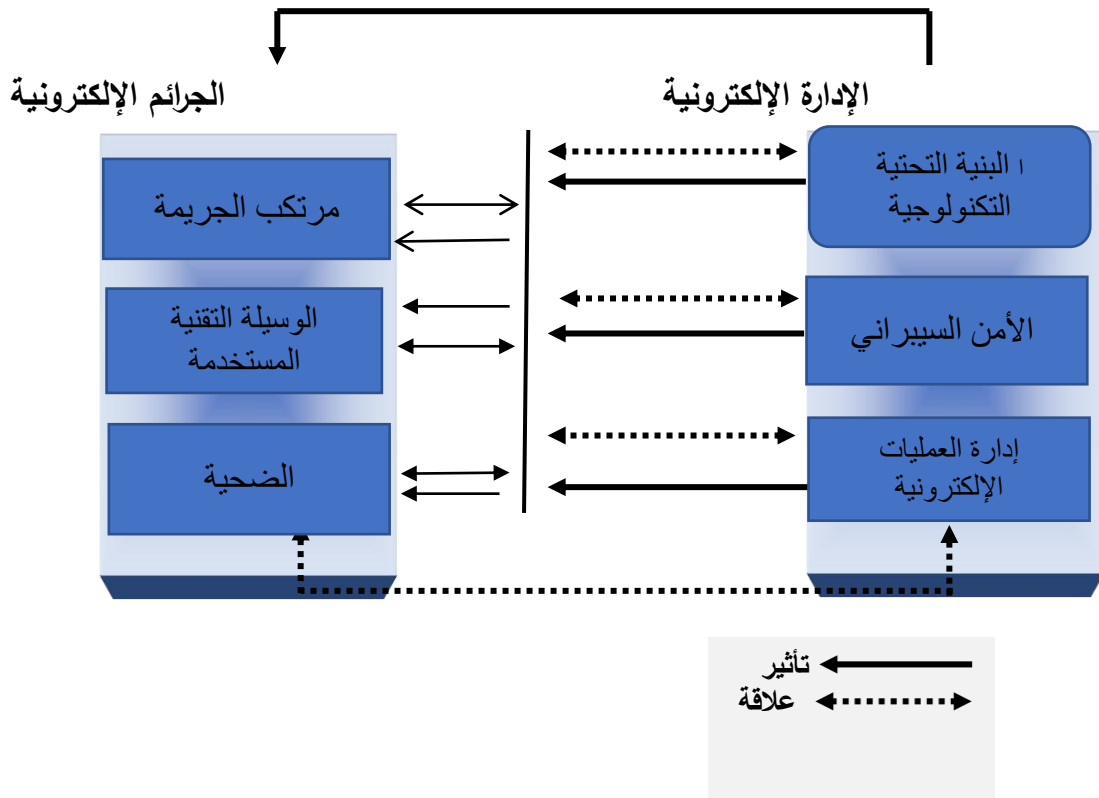
المبحث الرابع: الخاتمة (الاستنتاجات والتوصيات).

## ٦. النموذج الافتراضي للبحث:

من أجل تحقيق أهمية وأهداف البحث فقد وضع أنموذج افتراضي والذي تم الإشارة له الشكل

(١)، والذي بدوره يتضمن متغيرين هما:

- أ- المتغير المستقل: ويتمثل الإدارة الإلكترونية وأبعاده التي تتضمن (البنية التحتية التكنولوجية، الأمن السيبراني، إدارة العمليات الإلكترونية).
- ب- المتغير التابع: ويتمثل الجرائم الإلكترونية وأبعاده التي تتضمن (المرتكب الجريمة، الوسيلة التقنية المستخدمة، الضحية).



### المبحث الثاني: الجانب النظري في الدراسة

#### المطلب الأول: مفهوم وأهمية الإدارة الإلكترونية

##### ١. مفهوم الإدارة الإلكترونية (Concept of E-Administration)

تُعرف الإدارة الإلكترونية بأنها منظومة متكاملة تعتمد على استخدام التقنيات الرقمية والاتصالات الحديثة لتحويل العمل الإداري التقليدي (الورقي) إلى عمل رقمي، بهدف سرعة الإنجاز ورفع كفاءة الأداء وتقديم الخدمات للمواطنين بأقل جهد وتكلفة (سعد، ٢٠٢٥).

##### ٢. أهمية الإدارة الإلكترونية (Importance)

تتجلى أهمية الإدارة الإلكترونية في النقاط الآتية:  
تبسيط الإجراءات: تقليل الروتين الإداري والاعتماد على الأتمتة.



الشفافية والنزاهة: الحد من الفساد الإداري من خلال تقليل الاحتكاك المباشر بين الموظف والمواطن.

دقة البيانات: توفير قواعد بيانات مركزية تُسهل عملية اتخاذ القرار (ملاكدي واخرون، ٢٠٢٥).

### ٣. أهداف الإدارة الإلكترونية (Objectives)

رفع مستوى الرضا لدى المستفيدين من الخدمات الحكومية.

تقليل التكاليف التشغيلية الناتجة عن استخدام الأوراق والمخازن التقليدية.

تحقيق استجابة سريعة للمتغيرات التقنية العالمية. (بلوشى، ٢٠٢٣)

### ٤. خصائص الإدارة الإلكترونية (Characteristics)

تتميز الإدارة الإلكترونية في المؤسسات العراقية الحديثة بمجموعة من الخصائص التي تجعلها متفوقة على الإدارة التقليدية:

إلغاء الحواجز المكانية: إمكانية إنجاز المعاملات من أي مكان دون الحاجة للحضور الشخصي.

المرونة الزمنية: تقديم الخدمات على مدار الساعة (٧/٢٤) دون التقيد بأوقات الدوام الرسمي.

الاعتماد على المعرفة: تحويل البيانات إلى معلومات رقمية تُسهل عملية الرقابة والتدقيق. (الدرعي، ٢٠٢٢)

### ٥. متطلبات تطبيق الإدارة الإلكترونية (Requirements)

لكي تتجح عملية التحول الرقمي، لا بد من توفر المتطلبات الأساسية التالية:

المتطلبات التشريعية والقانونية: سن قوانين تحمي التعاملات الإلكترونية وتعتمد التوقيع الإلكتروني كحجة قانونية (مثل قانون التوقيع الإلكتروني العراقي المحدث).

المتطلبات البشرية: تدريب الموظفين وتطوير مهاراتهم الرقمية للتعامل مع الأنظمة الحديثة.

المتطلبات التقنية: توفر أجهزة الحاسوب، الخوادم (Servers)، وشبكات إنترنت فائقة السرعة ومستقرة.

المتطلبات المالية: تخصيص ميزانيات كافية لشراء البرمجيات وصيانة الأنظمة دورياً (المبارك والبحاري، ٢٠٢٥).

### المطلب الثاني: أبعاد الإدارة الإلكترونية

تعتمد كفاءة الإدارة الإلكترونية على ثلاثة أبعاد أساسية متداخلة، وهي:

### ١. البنية التحتية التكنولوجية (Technological Infrastructure)



تتمثل في المكونات المادية والبرمجية، وشبكات الاتصال المتطورة (مثل شبكة الألياف الضوئية في العراق). لا يمكن نجاح التحول الرقمي دون توفر خوادم (Servers) عملاقة وقواعد بيانات وطنية موحدة تربط المؤسسات ببعضها البعض

## ٢. الأمن السيبراني (Cybersecurity)

يعد الأمن السيبراني البعد الأكثر حرجاً، حيث يهدف إلى حماية البيانات الحكومية وشخصية المواطنين من الهجمات الإلكترونية والاختراقات. في العراق، تم التركيز مؤخراً على بناء "مركز الاستجابة للطوارئ المعلوماتية" لتأمين الفضاء الرقمي.

## ٣. إدارة عمليات إلكترونية (E-Operations Management)

يشير هذا البعد إلى إعادة هندسة العمليات الإدارية (BPR) لتتلاءم مع البيئة الرقمية، بدءاً من استقبال الطلب إلكترونياً، معالجته آلياً، وصولاً إلى تصدير النتيجة النهائية دون تدخل بشري مكثف (الشريف وآخرون، ٢٠٢٤).

## المطلب الثالث: مفهوم وأسباب الجرائم الإلكترونية

### ١. مفهوم الجرائم الإلكترونية (Concept of Cybercrime)

تُعرف الجريمة الإلكترونية بأنها أي نشاط غير مشروع يتم باستخدام الأجهزة الإلكترونية أو شبكات المعلومات (الإنترنت)، بهدف الوصول غير المصرح به للبيانات، أو تخريب الأنظمة، أو ابتزاز الأشخاص والمؤسسات مادياً ومعنوياً (محمد وآخرون، ٢٠٢٤).

### ٢. أسباب انتشار الجرائم الإلكترونية (Causes)

هناك عدة دوافع تقف وراء ارتكاب هذه الجرائم في البيئة العراقية، منها:  
الدوافع المادية: الرغبة في الحصول على الأموال بسرعة عبر الاحتيال المصرفي أو الابتزاز.  
الدوافع الانتقامية: تصفية حسابات شخصية أو مهنية من خلال تشويه السمعة الرقمية.  
ضعف الوعي التقني: عدم معرفة المستخدمين بطرق تأمين حساباتهم، مما يسهل اختراقها.  
الفراغ التشريعي السابق: الذي تمت معالجته مؤخراً بتشريعات أكثر صرامة (نصار، ٢٠٢٤).

### ٣. خصائص وأنواع الجرائم الإلكترونية (Characteristics & Types)

تتميز هذه الجرائم بأنها عابرة للحدود، صعبة الإثبات، وتتم بسرعة فائقة. ومن أهم أنواعها:  
الابتزاز الإلكتروني: وهو الأكثر شيوعاً في العراق حالياً.  
الاحتيال المالي: سرقة بيانات البطاقات المصرفية (مثل الماستركارد والكي كارد).  
الاختراق (Hacking): الدخول غير القانوني لقواعد البيانات الحكومية أو الخاصة (الدوري، ٢٠٢٤).



## الابتزاز الإلكتروني في العراق وإقليم كردستان

### ١. واقع الابتزاز الإلكتروني (Reality of Cyber-Extortion)

يعتبر الابتزاز الإلكتروني في العراق، وخاصة في إقليم كردستان، من أكثر الجرائم الرقمية نمواً في عامي ٢٠٢٤ و ٢٠٢٥. وتتمثل هذه الجريمة في تهديد الضحية بنشر صور أو معلومات خاصة مقابل مبالغ مالية أو تنازلات معينة، وقد سجلت مديريات مكافحة الإجرام في أربيل والسليمانية تصاعداً ملحوظاً في عدد الشكاوى المسجلة.

### ٢. الأطر القانونية والمواجهة (Legal Framework)

في إقليم كردستان، يتم التعامل مع هذه الجرائم وفقاً لـ "قانون سوء استخدام أجهزة الاتصالات"، بينما في المركز (بغداد)، يتم الاعتماد على مواد قانون العقوبات ومشروع قانون جرائم المعلوماتية الحديث، في عام ٢٠٢٤، تم تفعيل وحدات "الشرطة المجتمعية" و "السايبير" بشكل مكثف لتقديم الدعم التقني والقانوني للضحايا مع ضمان السرية التامة.

### ٣. التحديات الخاصة في البيئة المحلية

العادات والتقاليد: الخوف من "الفضيحة" يدفع الكثير من الضحايا (خاصة الإناث) إلى عدم التبليغ، مما يشجع المجرمين على الاستمرار.

التطور التقني للمجرمين: استخدام تقنيات "الذكاء الاصطناعي" و "التزييف العميق" (Deepfake) لتزوير صور ومقاطع فيديو غير حقيقية للضحايا (قانون رقم ٦ لسنة ٢٠٠٨).

### المطلب الرابع: أبعاد الجريمة الإلكترونية وسبل المواجهة

#### ١. أبعاد الجريمة الإلكترونية (Dimensions of Cybercrime)

تتكون الجريمة الإلكترونية من ثلاثة أركان أساسية (أبعاد) يجب تحليلها: مرتكب الجريمة: وغالباً ما يمتاز بالذكاء التقني، وقد يكون فرداً أو عصابة منظمة، ودوافعه تتراوح بين المادية والنفسية.

الوسيلة الإلكترونية: وهي الأداة المستخدمة (حاسوب، هاتف ذكي، شبكات التواصل الاجتماعي).

الضحية: قد يكون فرداً، مؤسسة مالية، أو حتى سيادة الدولة، وغالباً ما يتم استهداف الضحية عبر "الهندسة الاجتماعية".

#### ٢. النصوص القانونية (Legal Texts)

أ- في إقليم كردستان (قانون منع إساءة استعمال أجهزة الاتصالات رقم ٦ لسنة ٢٠٠٨):



ينص القانون في مادته الأولى على: "يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن مليون دينار ولا تزيد على خمسة ملايين دينار أو بإحدى هاتين العقوبتين كل من أساء استعمال أجهزة الهاتف الخليوي أو أجهزة الاتصال السلكية واللاسلكية أو الإنترنت... عن طريق التهديد أو الابتزاز أو نشر صور مخدشه للحياة".  
ب- في العراق الاتحادي (قانون العقوبات ١١ لسنة ١٩٦٩ وتعديلاته، ومشروع قانون مكافحة جرائم تقنية المعلومات ٢٠٢٤):

في جمهورية العراق الفدرالية ، ووفقا لقانون العقوبات العراقي وتعديلاته، تستند المحاكم حاليا الي المادتين (٤٣٠ و٤٥٢) في معالجة جرائم الابتزاز، واللتين تتضمنان عقوبات بالسجن والغرامة المالية، واستنادا الي مشروع (قانون جرائم المعلوماتية) الذي جرت عليه المناقشات النهائية في عام ٢٠٢٤، فقد تم اقتراح تشديد العقوبات، لتصل الي السجن المؤبد للجرائم التي تمس الأمن الوطني مع فرض عقوبات مغلظة بالسجن و غرامات مالية كبيرة لحالات الابتزاز الإلكتروني (الشخصي والمالي)، وقد نصت المادتان (١٨ و١٩) من المشروع علي تشديد عقوبة الابتزاز، و ذلك ضمن اطار مشروع القانون الجديد وتعديلات قانون العقوبات الرامية الي مكافحة الجرائم التقنية.

### ٣. طرق التغلب على الجرائم الإلكترونية (Prevention & Control)

لمواجهة هذه الظاهرة، يتطلب الأمر استراتيجية شاملة:  
المواجهة التقنية: استخدام برامج الحماية، التشفير القوي (Encryption)، وتفعيل التحقق بخطوتين (FA٢).  
المواجهة الأمنية: تعزيز دور وحدات "مكافحة الجرائم الإلكترونية" وتسهيل آليات التبليغ السري عبر الخطوط الساخنة (مثل الخط ١٠٤).  
التوعية المجتمعية: نشر ثقافة "الأمان الرقمي" وتدريب الكوادر الإدارية على كيفية التعامل مع الاختراقات. (الدويري، ٢٠٢٤)

### المبحث الثالث: الجانب التطبيقي في الدراسة

المطلب الأول: تحليل المعلومات الشخصية لأفراد عينة البحث

لجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء للمؤسسات الأمنية في مدينة السليمانية

إن الغرض من تحليل البيانات التي تم جمعها من خلال استخدام الاستبانة من إظهار مستويات إجابات أفراد عينة البحث فيما يتعلق بمتغيرات البحث، وتحقيقاً لهذا الغرض تم استخدام الأدوات الإحصائية

المناسبة مثل (التكرارات والنسب المئوية والأوساط الحسابية والانحرافات المعيارية)، لذا قام الباحثون بتوزيع (٦٧) استبيان بالطريقة العشوائية على المجتمع، وتم استردادها بالكامل بواقع (٥٧) استبيان، وبالتالي أصبحت الاستبيانات الصالحة للتحليل الإحصائي ما مجمله (٥٧) استبيان، وتم وصف وتشخيص خصائص أفراد وحدة العينة كما مبينة نتائجها بالجدول رقم (١).

الجدول (١) خصائص عينة البحث

الجنس										
انثى					ذكر					
النسبة		التكرار			النسبة		التكرار			
%28.1		16			%71.9		41			
العمر										
50 سنة فأكثر			41 - 50 سنة				34 - 40 سنة		أقل من 30 سنة	
النسبة		التكرار	النسبة		التكرار	النسبة		التكرار	التكرار	
%12.3		7	%31.6		18	%43.9		25	%12.3	7
عدد سنوات الخدمة										
16 سنة فأكثر			11 - 15 سنة		6 - 10 سنة		1 - 5 سنة		أقل من سنة	
النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	
26.3%	15	28.1%	16	15.8%	9	22.8%	13	7%	4	
التحصيل الدراسي										
دكتوراه			بكالوريوس		الدبلوم المهني		اعدادية		أقل من اعدادية	
النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	
28.1%	16	24.6%	14	14%	8	33.3%	19	0.00%	0	
عدد الدورات التدريبية في المجالات الادارية فقط										
ثلاث دورات فأكثر			دورتان تدريبيتان			دورة تدريبية واحدة			لم يشارك	
النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	
19.3%	11	14%	8	31.6%	18	35.1%	20			

الأخيرة. وجاءت بعدها عدد الدورات التدريبية الذين (لم يشارك في الدورة) بنسبة (٣٥.١%) وهذا يؤشر الى أكثرهم لم يشارك أي دورات إدارية أما من حيث عدد الدورات التدريبية للذين شاركوا في دورة تدريبية واحدة سجلت نسبة (٣١.٦%)، ويأتي أشخاص الذين

شاركت في ثلاث دورات فأكثر سجلت نسبة (19.3%)، ويأتي الأشخاص الذين شاركت في دورتان تدريبيتان سجلت نسبة (14%).

### المطلب الثاني: وصف وتشخيص متغيرات البحث

في ضوء استجابة وحدة المعاينة للمجتمع، سوف يتم الاعتماد على الوسط الحسابي والانحراف المعياري لتلك الإجابات. ولأن هذا البحث قد اعتمد على مقياس (Likert) الخماسي في إجابات عينة البحث للاستبيان، فسيكون مستوى كل متغير محصورا بين (1-5) بثلاث مستويات والجدول (2) يوضح ذلك، ويشتمل ثلاث مستويات عند الوسط المفترض البالغ (3).

### جدول (2) المتوسطات المرجحة لإجابات عينة البحث

المتوسط المرجح	مستوى التقييم
من 1 - لغاية 2.33	منخفض
من 2.34 - أقل من 3.67	متوسط
من 3.67 - لغاية 5	مرتفع

وكانت نتائج إجابات أفراد مجتمع الدراسة عن المتغيرات التي تناولتها الاستبيان، بناءً على تحليل تلك الإجابات المتعلقة بالمتغيرات كما يلي:

### أولاً: وصف وتشخيص الإدارة الإلكترونية

تم قياس هذا المتغير من خلال الأسئلة (1 - 15) والتي يمثل كل منها مكون 1 - 15 فقرة. فان الإجابة عن فقرات تلك الأبعاد اتجاهات عينة البحث ومدى تشخيصها في مجتمع للبحث. والجدول رقم (3) يبين ذلك:

### جدول رقم (3) نتائج وصف وتشخيص الإدارة الإلكترونية

الأبعاد	الفقرات	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	أهمية النسبية	المستوى القياس
الأول	البنية التحتية التكنولوجية					
1	البنية التحتية الإلكترونية في المؤسسة قوية بما يكفي لدعم العمليات الرقمية بكفاءة.	4.30	0.597	13.88%	85.96%	مرتفع
2	البنية التحتية الإلكترونية الحالية تسهم في تحسين أمان البيانات والمعلومات في المؤسسة.	4.28	0.620	14.48%	85.61%	مرتفع

لجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء  
للمؤسسات الأمنية في مدينة السليمانية



مرتفع	81.75%	14.08%	0.576	4.09	المؤسسة تستثمر بانتظام في تحديث وصيانة البنية التحتية الإلكترونية.	٣
مرتفع	80.35%	18.51%	0.744	4.02	البنية التحتية الإلكترونية تمكن المؤسسة من التكيف بسرعة مع التغيرات التكنولوجية.	٤
مرتفع	82.81%	16.73%	0.693	4.14	الاعتماد على بنية تحتية إلكترونية متطورة يقلل من المخاطر المتعلقة بالجرائم الإلكترونية.	٥
<b>الأمن السيبراني</b>						<b>الثاني</b>
مرتفع	82.11%	17.64%	0.724	4.11	المؤسسة تعتمد على استراتيجيات قوية للأمن السيبراني لحماية بياناتها الحساسة.	١
مرتفع	86.32%	16.48%	0.711	4.32	الأمن السيبراني يعد أولوية قصوى في جميع العمليات الإلكترونية للمؤسسة.	٢
مرتفع	80.70%	16.86%	0.680	4.04	المؤسسة تقدم تدريبات دورية للموظفين لزيادة الوعي بالأمن السيبراني.	٣
مرتفع	80.35%	16.63%	0.668	4.02	المؤسسة مجهزة جيداً لمواجهة التهديدات السيبرانية والتعامل مع الاختراقات الأمنية.	٤
مرتفع	80.20%	25.36%	1.017	4.01	تطبيقات الأمن السيبراني في المؤسسة تواكب أحدث التهديدات التكنولوجية.	٥
<b>إدارة العمليات الإلكترونية</b>						<b>الثالث</b>
مرتفع	84.60%	23.67%	1.001	4.23	إدارة العمليات الإلكترونية في المؤسسة تساهم في تحسين تدفق العمل وتقليل التعقيدات الإدارية.	١
مرتفع	82.20%	22.84%	0.939	4.11	المؤسسة تعتمد على نظام إدارة عمليات إلكترونية لتنسيق ومراقبة العمليات بفعالية.	٢



مرتفع	80.60%	21.04%	0.848	4.03	إدارة العمليات الإلكترونية تقلل من الأخطاء التشغيلية وتزيد من دقة العمليات.	٣
مرتفع	80.00%	20.05%	0.802	4.00	النظام الإلكتروني لإدارة العمليات يوفر تقارير فورية تساعد في اتخاذ قرارات مدروسة.	٤
مرتفع	79.40%	22.30%	0.885	3.97	إدارة العمليات الإلكترونية تساعد المؤسسة على التكيف بسرعة مع التغييرات في السوق والطلب.	٥
			0.7٧	4.1١	الإجمالي للمتغير	

#### المصدر: من إعداد الطلب بالاعتماد على نتائج البحث

نلاحظ من خلال النتائج الظاهرة في الجدول (٣) تم قياس هذا المتغير من خلال ثلاث ابعاد فرعية، وقد بلغ الوسط الحسابي الإجمالي الموزون الإدارة الإلكترونية (٤.١١) وهو أكبر من الوسط الفرضي البالغ (٣) وبانحراف معياري (٠.٧٧) يشير الى ان الإدارة الإلكترونية في العينة الدراسة جاء بمستوى مرتفعة بحسب أجابتهم على فقرات الاستبانة.

#### ثانياً: وصف وتشخيص الجرائم الإلكترونية والتكنولوجية

قد تم قياس هذا المتغير من خلال الفقرات (١ - ١٥) والتي يمثل كل منها مكونا الجرائم الإلكترونية وبالتالي فإن الإجابة عن هذه المقاييس الفرعية تعكس اتجاهات عينة البحث ومدى تشخيصها للأداء، وكما مبينة نتائجها بالجدول أدناه.

#### جدول رقم (٤) نتائج وصف وتشخيص الجرائم الإلكترونية

الابعاد	الفقرات	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	أهمية النسبية	المستوى القياس
الاول	مرتكب الجريمة					
١	مرتكبو الجرائم الإلكترونية غالباً ما يستغلون الثغرات الأمنية في أنظمة المؤسسة.	3.63	0.975	26.85%	72.63%	مرتفع

الجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء  
للمؤسسات الأمنية في مدينة السليمانية



مرتفع	84.91%	13.56%	0.576	4.25	معظم مرتكبي الجرائم الإلكترونية يتمتعون بمستوى عالٍ من المهارات التقنية والمعرفة الرقمية.	٢
مرتفع	85.26%	13.68%	0.583	4.26	الدوافع الرئيسية لمرتكبي الجرائم الإلكترونية تشمل الربح المالي والوصول غير المصرح به إلى المعلومات الحساسة.	٣
مرتفع	84.56%	14.84%	0.627	4.23	مرتكبو الجرائم الإلكترونية غالباً ما يستهدفون المؤسسات ذات الدفاعات الإلكترونية الضعيفة.	٤
مرتفع	85.26%	15.69%	0.669	4.26	تتزايد قدرة مرتكبي الجرائم الإلكترونية على الابتكار وتطوير أساليب جديدة للاختراق.	٥
الوسيلة الإلكترونية المستخدمة						الثاني
مرتفع	86.32%	13.25%	0.572	4.32	مرتكبو الجرائم الإلكترونية يعتمدون على برمجيات خبيثة لاختراق أنظمة الحماية في المؤسسات.	١
مرتفع	88.42%	13.48%	0.596	4.42	التصيد الاحتيالي هو	٢



لجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء  
للمؤسسات الأمنية في مدينة السليمانية

					إحدى الوسائل الأكثر شيوعاً في تنفيذ الجرائم الإلكترونية.	
مرتفع	86.67%	14.68%	0.636	4.33	تستخدم الجرائم الإلكترونية تقنيات تشفير متقدمة لإخفاء هوية المهاجمين.	٣
مرتفع	87.72%	17.64%	0.774	4.39	الهجمات على الشبكات اللاسلكية (Wi-Fi) تُعد وسيلة شائعة لاختراق الأجهزة والأنظمة.	٤
مرتفع	86.32%	17.60%	0.760	4.32	التقنيات المتقدمة مثل الذكاء الاصطناعي تُستخدم في تطوير أدوات هجومية جديدة في الجرائم الإلكترونية.	٥
الضحية						الثالث
مرتفع	83.86%	17.71%	0.743	4.19	أشعر أن الوعي بالتهديدات الإلكترونية مهم جداً لحماية نفسي من الجرائم الإلكترونية.	١
مرتفع	81.40%	20.16%	0.821	4.07	يتأثر الجرائم الإلكترونية على ضحاياها يمكن أن يكون مدمراً على المدى الطويل.	٢
مرتفع	84.56%	18.44%	0.780	4.23	أن الضحايا غالباً ما يشعرون بالعزلة بعد تعرضهم للجرائم	٣



الجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء  
للمؤسسات الأمنية في مدينة السليمانية



الإلكترونية.					
المؤسسات الأمنية تعمل جهودا كبيرا لمساعدة ضحايا الجرائم الإلكترونية كافية ومناسبة.	4.16	0.676	16.25%	83.16%	مرتفع
المؤسسات الأمنية تعمل للضحايا الذين تلقوا دعماً نفسياً أن يتعافوا بشكل أفضل من آثار الجرائم الإلكترونية.	4.17	0.683	16.38%	83.40%	مرتفع
الإجمالي للمتغير	4.22	0.70			

المصدر: من إعداد الباحث بالاعتماد على نتائج البحث

نلاحظ من خلال النتائج الظاهرة في الجدول (٤) تم قياس هذا المتغير من خلال ١ - ١٥ فقرة، وقد بلغ الوسط الحسابي الموزون ل (الجرائم الإلكترونية) (٤.٢٢) وهو أكبر من الوسط الفرضي البالغ (٣) وبانحراف معياري (٠.٧٠) مما يشير الى الجرائم الإلكترونية محل البحث بدرجة مرتفعة بحسب إجابتهم على فقرات الاستبانة.

المطلب الثالث: عرض نتائج التحليل

أولاً: اختبار فرضية الارتباط

الفرضية الرئيسية الأولى: توجد علاقة ارتباط معنوية بين الجرائم الإلكترونية والإدارة الإلكترونية.

لمعرفة العلاقة الارتباطية بين متغيرات البحث المتغير المستقل والمتمثل (الإدارة الإلكترونية) مع المتغير المعتمد والمتمثل في (الجرائم الإلكترونية والتكنولوجية) تم استخدام معامل ارتباط بيرسون وكانت النتائج كما في جدول مما يلي: جدول رقم (٥)

العلاقة بين الابعاد (الإدارة الإلكترونية)	الجرائم الإلكترونية والتكنولوجية
الارتباط	الدلالة الإحصائية



0.000 **	0.691	البنية التحتية التكنولوجية
0.000 **	0.573	الأمن السيبراني
0.000 **	0.673	إدارة العمليات الإلكترونية
0.000 **	0.737	الإجمالي للمتغير (الإدارة الإلكترونية)

المصدر: من إعداد الباحث اعتماداً على نتائج التحليل؛ (\*\*) معنوية عند (0.01) (\*) معنوية عند (0.05).

نلاحظ من نتائج الجدول (5) ان هناك ارتباط بين الإدارة الإلكترونية وأبعادها مع الجرائم الإلكترونية إذ بلغ معامل الارتباط للمتغير الإدارة الإلكترونية (0.737) وإبعادها (البنية التحتية التكنولوجية والأمن السيبراني وإدارة العمليات الإلكترونية) على التوالي كلها معنوية مقارنة مستوى دلالة الإحصائية مع مستويات المعنوية (0.01, 0.05) وهي أقل، وكانت العلاقة إيجابية وتشير تلك القيمة الموجبة الى العلاقة الطردية بين المتغيرين وهذا يؤكد ميل العلاقة للزيادة المتغيرين وبالتالي تقبل الفرضية الرئيسية الأولى والفرضيات بصيغة الأثبات.

#### ثانياً: اختبار فرضية التأثير

تم اختبار هذه الفرضية في البحث المتعلقة بقياس تأثير المتغير المستقل في المتغير التابع باستخدام نموذج الانحدار الخطي البسيط ولأجل ذلك فقد وضعت فرضية رئيسة لتحليل علاقة التأثير بين المتغير المستقل والمتغير التابع وهي كما يلي:

الفرضية الرئيسية الثانية: يوجد تأثير معنوي الإدارة الإلكترونية في الجرائم الإلكترونية والتكنولوجية.

الجدول (٦) نتائج تقدير العلاقة والتأثير

المتغير التابع						الارتباط
البنية التحتية التكنولوجية	الأمن السيبراني	إدارة العمليات الإلكترونية	الإجمالي للمتغير (الإدارة الإلكترونية)	المتغير المستقل	المتغير التابع	الارتباط
0.000	0.000	0.000	0.000	0.744	0.691	0.477
0.000	0.000	0.000	0.000	0.528	0.573	0.328

السيبراني						
إدارة العمليات الإلكترونية	0.000	6.748	0.523	0.000	45.535	0.453
الإجمالي للمتغير المستقل (الإدارة الإلكترونية)	0.000**	8.087	0.670	0.000**	65.395	0.543

المصدر: من إعداد الباحث اعتماداً على نتائج التحليل؛ (\*\*) معنوية عند (0.01) (\*) معنوية عند (0.05).

وكما نلاحظ من النتائج الظاهرة في الجدول ( ٦ ) ان الفرضية الرئيسية الثانية التي مفادها هناك تأثير معنوي للمتغير الإدارة الإلكترونية و ابعادها (البنية التحتية التكنولوجية و الأمن السيبراني و إدارة العمليات الإلكترونية ) على التوالي في الجرائم الإلكترونية و التكنولوجية قد تحققت، حيث بلغت قيمة (F) المحسوبة (65.395 و 50.109، 26.885، 45.035) على التوالي وهي معنوية مقارنة بين قيمة الدلالة الإحصائية اقل من مستوى المعنوي (0.05) وهذا يدل على معنوية العلاقة المفترضة بين المتغير المستقل والمتغير التابع، كما يشير معامل التحديد ( $R^2$ ) الى ان الإدارة الإلكترونية و ابعادها (البنية التحتية التكنولوجية و الأمن السيبراني و إدارة العمليات الإلكترونية ) على التوالي يفسر ما مقداره (54.3%، 47.7%، 32.8%، 45.3%) على التوالي من التغيرات التي تحصل في العينة محل الدراسة، ونظراً على اختبار ميل الانحدار باختبار (t) و قيمة دلالة اختبار (0.000) وهي معنوية مقارنة بين قيمة الدلالة الإحصائية اقل من مستوى المعنوي (0.05) وهذا يدل على معنوية العلاقة المفترضة وتشير تلك النتائج الى معنوية علاقة التأثير بين المتغيرين محل البحث التي تمتاز الإدارة الإلكترونية و ابعادها (البنية التحتية التكنولوجية و الأمن السيبراني و إدارة العمليات الإلكترونية ) على التوالي لها تأثيراً معنوياً في الجرائم الإلكترونية و التكنولوجية، وبالتالي تقبل الفرضية الرئيسية الثانية بصيغة الاثبات.

المبحث الرابع: الخاتمة

خلصت الدراسة إلى ضرورة استخدام المؤسسات الأمنية لأنظمة إدارة المعلومات الاستخباراتية للسيطرة على الجرائم قبل وقوعها، وتسلط الضوء على مخاطر الاختراق الإلكتروني على المؤسسات الحكومية والأمنية، وكيف يُمكن للإدارة الفعالة أن تمنعه. ونتيجة لهذا التحليل، توصلنا نظرياً وعملياً إلى الاستنتاجات التالية، ولهذا السبب قدمنا التوصيات

**أولاً: الاستنتاجات (Conclusions):** أن التحول نحو الإدارة الإلكترونية ضرورة حتمية لرفع كفاءة المؤسسات وتقليل الفساد المالي والإداري، هناك علاقة طردية بين التطور التقني وزيادة مخاطر الجرائم الإلكترونية، مما يتطلب توازناً بين "التحديث" و"التأمين"، أثبتت القوانين المعمول بها في إقليم كردستان والعراق فاعليتها، لكنها تحتاج إلى تحديث مستمر لمواكبة تقنيات الذكاء الاصطناعي.

من خلال دراسة الإدارة الإلكترونية وعلاقتها بالجرائم الإلكترونية في البيئة العراقية، توصلنا إلى النتائج الآتية:

١. العلاقة بين الإدارة الإلكترونية والجرائم الإلكترونية: من خلال التحليل الإحصائي باستخدام معامل ارتباط بيرسون، تبين وجود علاقة طردية بين الإدارة الإلكترونية والجرائم الإلكترونية، حيث أن تحسين البنية التحتية الإلكترونية يعزز من حماية المؤسسة، وبالتالي يقلل من احتمالية حدوث الجرائم الإلكترونية.

٢. أهمية البنية التحتية التكنولوجية: أظهرت النتائج أن المؤسسات التي تمتلك بنية تحتية إلكترونية قوية تتمتع بمستوى أمان أعلى، ما يسهم في تقليل التهديدات الإلكترونية ويحسن من أمان البيانات والمعلومات الحساسة.

٣. الأمن السيبراني ودوره في تقليل التهديدات: أكدت النتائج أن تطبيق استراتيجيات أمن سيبراني قوية يعد أولوية قصوى للمؤسسات التي تهدف لحماية بياناتها الحساسة، تلك الاستراتيجيات تقلل من فرص حدوث اختراقات أمنية أو سرقات معلومات.

٤. استخدام التقنيات المتقدمة في الجرائم الإلكترونية: تم التوصل إلى أن الجرائم الإلكترونية تزداد تعقيداً مع استخدام التقنيات المتقدمة مثل الذكاء الاصطناعي، ما يجعل اكتشاف الجرائم ومواجهتها أكثر تحدياً للمؤسسات.

٥. تحسين العمل عبر الإدارة الإلكترونية: إدارة العمليات الإلكترونية تساعد المؤسسات في تحسين تدفق العمل وتقليل التعقيدات الإدارية، وهو ما يقلل من الأخطاء التشغيلية ويزيد من دقة العمليات، كما يساعد في اتخاذ قرارات مبنية على بيانات فورية.





٦. الوعي بالجرائم الإلكترونية بين المشاركين: أظهرت الدراسة أن مستوى الوعي بالجرائم الإلكترونية بين أفراد العينة مرتفع، مما يعكس إدراكهم للمخاطر المرتبطة بالجرائم الإلكترونية والحاجة لاتخاذ إجراءات وقائية.

**ثانياً: التوصيات (Recommendations):** بناءً على ما تقدم، نوصي بالآتي:

١. الاستثمار في تحديث البنية التحتية التكنولوجية (في الأمن السيبراني): ضرورة تخصيص ميزانيات مستقلة لحماية قواعد البيانات الوطنية من الاختراق ينصح المؤسسات بالاستثمار المستمر في تحديث وصيانة بنيتها التحتية التكنولوجية، لضمان قدرتها على مواجهة التهديدات الإلكترونية المتطورة وتقليل احتمالية تعرضها للاختراقات.

٢. تدريب الموظفين على استراتيجيات الأمن السيبراني (التوعية القانونية): يُوصى بتقديم تدريبات دورية للموظفين لزيادة الوعي بالأمن السيبراني، وضمان استعدادهم للتعامل مع التهديدات السيبرانية بطريقة فعالة. هذا يشمل التعرف على أساليب الهجمات الشائعة مثل التصيد الاحتيالي.

٣. رفع الوعي بأساليب الجرائم الإلكترونية: يُنصح المؤسسات بتنفيذ حملات توعية داخلية حول أساليب الجرائم الإلكترونية مثل التصيد الاحتيالي والبرمجيات الخبيثة، لضمان أن جميع الموظفين على دراية بالمخاطر وكيفية تجنبها.

٤. اعتماد تقنيات متقدمة للأمن الإلكتروني: يجب أن تسعى المؤسسات إلى تبني تقنيات حديثة مثل الذكاء الاصطناعي للتنبؤ بالهجمات الإلكترونية واكتشاف التهديدات بشكل مبكر، مما يقلل من تأثير الجرائم الإلكترونية.

٥. تعزيز السياسات الأمنية في المؤسسة: من المهم تنفيذ سياسات صارمة لتعزيز الأمن الإلكتروني، مثل إجراء اختبارات دورية على الأنظمة والبنية التحتية، ومراقبة الأنشطة الشبكية بشكل مستمر لتجنب أي محاولات اختراق.

٦. دعم ضحايا الجرائم الإلكترونية: يُنصح بتعزيز التعاون مع الجهات الأمنية لتوفير الدعم النفسي والتقني لضحايا الجرائم الإلكترونية، مما يساهم في تقليل الآثار النفسية والتقنية طويلة الأمد التي قد تؤثر على أداؤهم داخل المؤسسة.

٧. تطوير البنية التحتية: الإسراع في إكمال المشاريع الرقمية (مثل البطاقة الوطنية والخدمات المصرفية الشاملة) لتقليل التعاملات الورقية.

٨. ينبغي على المشرعين صياغة نصّ قانوني واضح يُعرّف ويُحدّد حالات الخطر قبل ارتكاب الجريمة.



لجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء  
للمؤسسات الأمنية في مدينة السليمانية

٩. ينبغي على المشرّعين والباحثين الذين حدّدوا عوامل الخطر الإجرامية إضافة عوامل خطر جديدة وحديثة.

١٠. ينبغي اتباع المنهج العلمي القائم على التحقيق المنهجي مع الجاني لتسهيل الكشف عن الخطر الإجرامي.

١١. ينبغي مواجهة الخطر الإجرامي لمجرمي الإنترنت من خلال الحبس أو الغرامات أو أي إجراءات أمنية تحد من الخطر.

١٢. سنّ قوانين تدابير خاصة تتناسب مع طبيعة وخطورة جرائم المعلوماتية، بحيث تتميز بسرعة التنفيذ ومحو آثارها، والتأكد من أن قوانين التحقيق تشمل فعالية وضبط الأدلة الرقمية وكل ما يُساعد في التحقيقات.

١٣. وأخيراً، ندعو ضحايا جرائم المعلوماتية إلى الإبلاغ عن هذه الجرائم وتقديم الشكاوى والبلاغات إلى أجهزة وخدمات الشرطة القضائية ومعاونيهم والأجهزة الأمنية في عملية التحقيق.

المصادر (References):

المصادر العربية والكردية (مجلة وكتب): -

١. برلمان إقليم كردستان-العراق (٢٠٠٨). قانون رقم (٦) لسنة ٢٠٠٨: قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كردستان-العراق، الصادر بتاريخ ١٩/٥/٢٠٠٨، منشور في جريدة وقائع كردستان، العدد (٨٩)، بتاريخ ١٢/٦/٢٠٠٨.

٢. بلوشي، حنان يوسف ميرزا ٢٠٢٣. متطلبات تحقيق الإدارة الإلكترونية بجامعة الكويت. مجلة كلية التربية - جامعة المنصورة، العدد ١٢٤.

٣. الدرعي، حميد راشد عبيد ٢٠٢٢. متطلبات تطوير الإدارة الإلكترونية لرفع الكفاءة المهنية لمديري مدارس الحلقة الثالثة بإمارة أبو ظبي. مجلة كلية التربية - جامعة المنصورة، العدد ١٢٠.

٤. الدويري، فراس عقيل علي ٢٠٢٤. البيانات الضخمة ودورها في الحد من الجرائم الإلكترونية في ظل إستراتيجية الأمن السيبراني. عمان: دار وائل للنشر والتوزيع.

٥. سعد، ياسين غالب ٢٠٢٥. الإدارة الإلكترونية وأفاق تطبيقاتها العربية. السعودية: الإدارة العامة للنشر والتوزيع.

٦. سليمان، أماني وفلاح، مها ٢٠٢٥. دور الإدارة الإلكترونية في تحقيق التمكين الإداري - دراسة حالة شركة يونتشارم الخليج لسنة ٢٠٢٥م. كلية إدارة الأعمال، جامعة نجران.

٧. الشريف، عمر احمد أبو هاشم، وعبد العليم، أسامة محمد، وبيومي، هشام محمد ٢٠٢٤. الإدارة الإلكترونية: مدخل الي الإدارة التعليمية الحديثة. دار المناهج للنشر والتوزيع.

٨. عبدو، محمد على الطاهر ٢٠١٩. متطلبات تطبيق الإدارة الإلكترونية في كلية الاقتصاد والمحاسبة بجامعة سبها. مجلة البحوث الأكاديمية، العدد ١٣.



لجرائم الإلكترونية والسيطرة عليها من خلال الإدارة الإلكترونية الفعالة. دراسة ميدانية حول آراء  
للمؤسسات الأمنية في مدينة السليمانية



- ٩.المبارك، فهد والبحاري، حامد ٢٠٢٥. أثر التحول الرقمي على كفاءة العمليات الإدارية في المؤسسات الحكومية. المجلة الدولية للعلوم المالية والإدارية والاقتصادية، ٤(١١).
- ١٠.محمد، أمال جمعة عبد الفتاح، والسالمية، ليلى، وجبر، أحلام عبد الستار ٢٠٢٤. الجرائم الإلكترونية: آفة الألفية الثالثة. القاهرة: مكتبة الأنجلو المصرية.
- ١١.ملاكدي، ح. ي.، القباطي، ح. ع.، العبسي، ج. ج.، عبدالله، ط. ع.، والنهاري، ع. م. ٢٠٢٥. الإدارة الإلكترونية ودورها في تحسين الأداء الوظيفي. مجلة تهامة، ١١(٢١).
- ١٢.نجم، عيود ٢٠٠٤. الإدارة الإلكترونية. دار المريخ للنشر.
- ١٣.نصار، غادة ٢٠٢٤. الجريمة الإلكترونية في المجتمع المصري: الأسباب والمواجهة. القاهرة: دار النهضة العربية.

ثانياً: المصادر المترجمة والأجنبية (English References) :-

- 1.Al-Shaboul, R., Ghneimat, R. and Al-Smadi, M. 2014. Challenges and factors affecting the implementation of e-government in Jordan. Journal of Software Engineering and Applications, 7(13), pp. 1111-1127.
- 2.Brenner, S.W. 2010. Cyberthreats: The Criminal Capabilities of Digital Technologies. Praeger.
- 3.Davenport, T.H. and Ronanki, R. 2018. Artificial Intelligence for the Real World. Harvard Business Review, 96(1), pp. 108-116.
- 4.Gil-Garcia, J.R., Dawes, S.S. and Pardo, T.A. 2018. Digital government and public management research. Public Management Review, 20(5), pp. 633-646.
- 5.Gil-Garcia, J.R., Pardo, T.A. and Gasco-Hernandez, M. (2018) Beyond Smart Cities: How Cities Network, Learn and Innovate. 1st edn. London: Springer Nature.
- 6.Holt, T.J., Bossler, A.M. and Seigfried-Spellar, K.C. 2018. Cybercrime and Digital Forensics: An Introduction. 2nd edn. London: Routledge.
- 7.Kshetri, N. 2021. Cybercrime and Cybersecurity in the Global Digital Economy. Computer, 54(4), pp. 82-87.
- 8.Kshetri, N. (2021) The Economics of Cybersecurity: A Strategic Management View. 1st edn. Berlin: Springer Nature
- 9.Mergel, I., Edelman, N. and Haug, N. 2019. Defining digital transformation: Results from expert interviews. Government Information Quarterly, 36(4), 101385.
- 10.Wall, D.S. 2017. Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
- 11.Yar, M. and Steinmetz, K.F. 2019. Cybercrime and Society. 3rd edn. SAGE Publications.

