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

م. م. صبريه كريم خالند
جامعة السليمانية التقنية، معهد التقني بكرجو،
قسم الإدارة الإلكترونية
sabria.khaland@spu.edu.iq

أ. م. عمر مصطفى محمد
جامعة السليمانية التقنية، معهد التقني دوكان،
قسم الإدارة الأعمال
Omer.mustafa@spu.edu.iq

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

كيفية اقتباس البحث

خالند، 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، نيسان٢٠٢٦، المجلد:١٦ ،العدد:٤ .

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

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 Khaland
Sulaimani Polytechnic University, Bakrjo Technical Institute, Department of E-Management

Assistant Professor
Omar Mustafa Mohammed
Sulaimani Polytechnic University, Dokan Technical Institute, Department of Business Administration

Keywords : E-Administration ؛Cybercrime ؛Cybersecurity ؛Cyber-Extortion ؛Digital Transformation

How To Cite This Article
Khaland, : 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.

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 فعّالة وسياسات أمن سيبراني ضرورة ملحة لمكافحة هذه التهديدات.

أُجري البحث على شكل دراسة وصفية تحليلية، وكانت الاستبانة المنظمة هي الأداة الرئيسية لجمع البيانات. وُزِّعت الاستبانة على عينة عشوائية مكونة من ٦٧ مديرًا ومسؤولًا وموظفًا يعملون في المؤسسات الأمنية بمدينة السليمانية، وجُمعت ٥٧ استجابة صالحة وخضعت للتحليل، وقُيّمت 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 تغييرًا جذريًا في كيفية إدارة المؤسسات لوظائفها الإدارية وتقديم خدماتها. وقد شهدت التقنيات الرقمية بروز الإدارة الإلكترونية التي تُمكّن 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).

تُمكّن 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. تُعرَّف 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 تعقيدًا 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 أطرًا 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 التهديدات الإلكترونية (برينر، ٢٠١٠؛ وول، ٢٠١٧). وبالتالي، يُعدّ تطبيق أنظمة إدارة إلكترونية ناجحة مع أمن سيبراني فعال أمرًا 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 عالميًا. 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;Kshertri,2021).

أصبحت الجرائم الإلكترونية تحديًا خطيرًا للمؤسسات، نظرًا 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 الأمن السيبراني، ومحدودية وعي الموظفين بالتهديدات الإلكترونية، ونقص التكامل بين الأنظمة الإدارية واستراتيجيات الأمن 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 –المتمثلة 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 الفعّالة 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 وُزِّع 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).

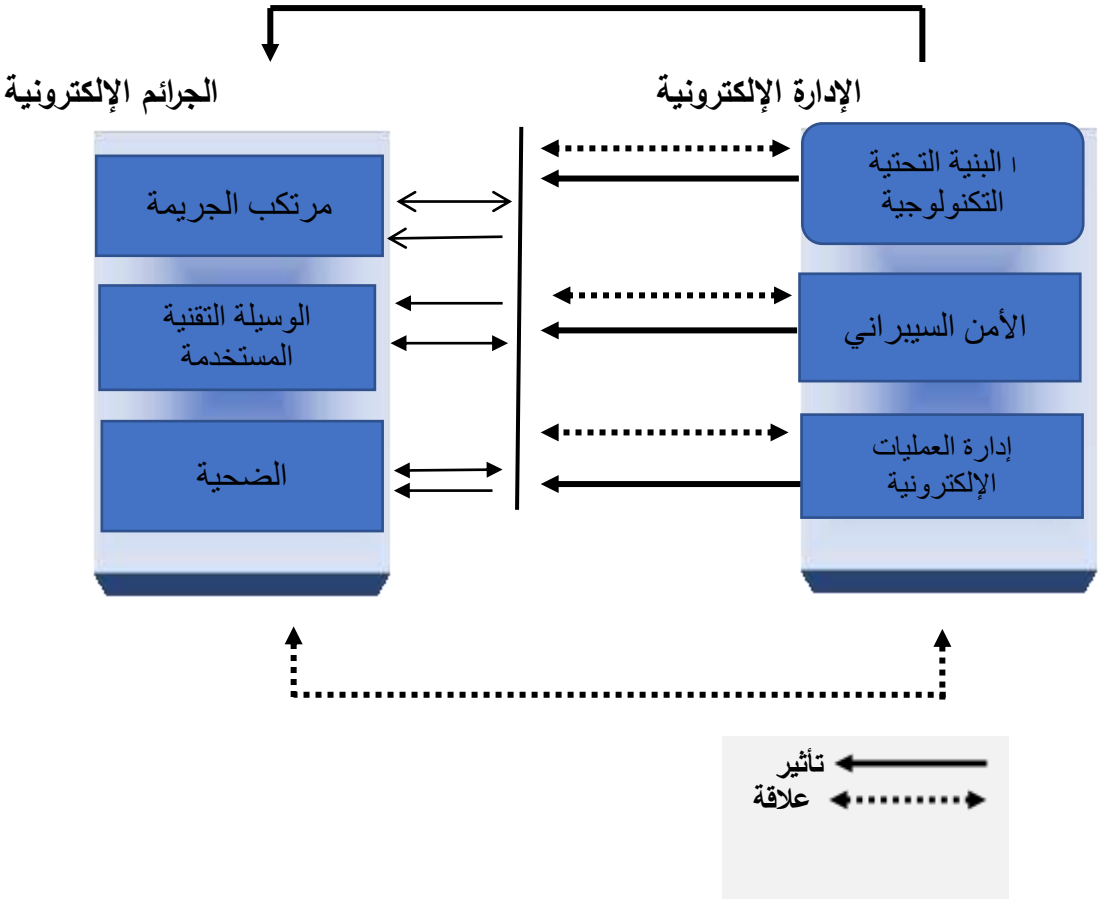
المبحث الرابع: الخاتمة (الاستنتاجات والتوصيات).

٦.النموذج الافتراضي للبحث:

من اجل 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 (ملاكدى 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. (الدرعى،٢٠٢٢)

٥.متطلبات تطبيق الإدارة الإلكترونية (Requirements)

لكي تنجح 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 واخرون،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 واخرون،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 كوردستان

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

يعتبر الابتزاز الإلكتروني في العراق، وخاصة في إقليم كوردستان، من أكثر الجرائم الرقمية نمواً في عامي ٢٠٢٤ و٢٠٢٥. 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 كوردستان، 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" السايبر" 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 كوردستان (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 الخلوي أو أجهزة الاتصال السلكية واللاسلكية أو الإنترنت... عن طريق التهديد أو الابتزاز أو نشر صور مخدشه للحياء".

ب- في العراق الاتحادي (قانون العقوبات ١١١لسنة ١٩٦٩وتعديلاته، ومشروع قانون مكافحة جرائم تقنية المعلومات ٢٠٢٤):

في جمهورية العراق الفدرالية ، ووفقا لقانون العقوبات العراقي وتعديلاته، تستند المحاكم حاليا الي المادتين(٤٣٠و٤٥٢) في معالجة جرائم الابتزاز، واللتين تتضمنان عقوبات بالسجن والغرامة المالية، واستنادا الي مشروع(قانون جرائم المعلوماتية)الذي جرت علية 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(١٨و١٩) 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

إن الغرض من تحليل البيانات التي تم جمعها من خلال استخدام الاستبانة من إظهار مستويات إجابات أفراد عينة البحث فيما يتعلق بمتغيرات البحث، وتحقيقا 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			
ذكر		انثى	
التكرار	النسبة	التكرار	النسبة
41	%71.9	16	%28.1

العمر							
أقل من 30 سنة		30 – 40 سنة		41 – 50 سنة		50 سنة فأكثر	
التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة
7	%12.3	25	%43.9	18	%31.6	7	%12.3

عدد سنوات الخدمة									
أقل من سنة		1— 5 سنة		6 – 10 سنة		11— 15 سنة		16سنة فأكثر	
التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة
4	%7	13	22.8%	9	15.8%	16	28.1%	15	26.3 %

التحصيل الدراسي									
أقل من اعدادية		اعدادية		الدبلوم المهني		بكالوريوس		دكتوراه	
التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة
0	0.00%	19	33.3%	8	14%	14	24.6%	16	28.1%

عدد الدورات التدريبية في المجالات الادارية فقط							
لم أشارك		دورة تدريبية واحدة		دورتان تدريبيتان		ثلاث دورات فأكثر	
التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة
20	35.1 %	18	31.6%	8	14%	11	19.3%

المصدر: من إعداد الباحث بالاعتماد على نتائج البحث

نلاحظ من نتائج الجدول (١)إن فئة الذكور شكلت معدلا أكبر من الإناث بنسبة (٧١.٦%) إما نسبة الإناث فشكلت (٢٨.١%) وهذا يدل على ان نسبة الذكور أكبر من نسبة الإناث في مجتمع البحث. وجاءت الفئات العمرية ان أكبر نسبة كانت من الفئات العمرية من (٣٠ – ٤٠) بواقع (٤٣.٩%)، أما بالنسبة لفئة العُمر (٤١ – ٤٠)نسبتهم (٣١.٦%)، يأتي الفئة العمرية (أقل من ٣٠ سنة و٥٠ سنة فأكثر) بنسبة (١٢.٣%) كل فئة على حدا. أما من ناحية عدد سنوات الخدمة نرى ان من لديهم سنوات الخدمة (١١ – ١٥ سنة) هم يشكلون ما يقارب (٢٨.١%) وتليها سنوات الخدمة (١٦ سنة فأكثر) بنسبة (٢٦.٣%) وتليها سنوات الخدمة (١ – ٥ سنة) بنسبة (٢٢.٨%) وتليها سنوات الخدمة (٦ –١٠ سنة) بنسبة (١٥.٨%) وتليها سنوات الخدمة (أقل من سنة) بنسبة (٧%). وجاءت بعدها التحصيل الدراسي من (إعدادية) بنسبة (٣٣.٣%) وهذا يؤشر الى أكثرهم إعدادية أما من حيث التحصيل الدراسي (دكتوراه)سجلت نسبة (٢٨.١%) أما من حيث التحصيل الدراسي (بكالوريوس) سجلت نسبة (٢٤.٦%) أما من حيث التحصيل الدراسي (الدبلوم المهني) سجلت نسبة (١٤%) بالمرتبة 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 (١٩.٣%)، ويأتي الأشخاص الذين شاركت في دورتان تدريبيتان سجلت نسبة (١٤%).

المطلب الثاني: وصف وتشخيص متغيرات البحث

في ضوء استجابة وحدة المعاينة للمجتمع، سوف يتم الاعتماد على الوسط الحسابي والانحراف المعياري لتلك الإجابات. ولان هذا البحث قد اعتمد على مقياس (Likert) الخماسي في إجابات عينة البحث للاستبيان، فسيكون مستوى كل متغير محصورا بين (5–1) بثلاث مستويات والجدول (٢) يوضح ذلك، ويشتمل ثلاث مستويات عند الوسط المفترض البالغ (٣).

جدول (٢) 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:

أولا: وصف وتشخيص الإدارة الإلكترونية

تم قياس هذا المتغير من خلال الأسئلة (١ – ١٥) والتي يمثل كل منها مكون ١ – ١٥ فقرة فان الإجابة عن فقرات تلك الابعاد اتجاهات عينة البحث ومدى تشخيصها في مجتمع للبحث. والجدول رقم (٣) يبين ذلك:

جدول رقم (٣) نتائج وصف وتشخيص الإدارة الإلكترونية

الابعاد	الفقرات	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	أهمية النسبية	المستوى القياس
الأول	البنية التحتية التكنلوجية					
١	البنية التحتية الإلكترونية في المؤسسة قوية بما يكفي لدعم العمليات الرقمية بكفاءة.	4.30	0.597	13.88%	85.96%	مرتفع
٢	البنية التحتية الإلكترونية الحالية تسهم في تحسين أمان البيانات والمعلومات في المؤسسة.	4.28	0.620	14.48%	85.61%	مرتفع
٣	المؤسسة تستثمر بانتظام في تحديث وصيانة البنية التحتية الإلكترونية.	4.09	0.576	14.08%	81.75%	مرتفع
٤	البنية التحتية الإلكترونية تمكن المؤسسة من التكيف بسرعة مع التغيرات التكنولوجية.	4.02	0.744	18.51%	80.35%	مرتفع
٥	الاعتماد على بنية تحتية إلكترونية متطورة يقلل من المخاطر المتعلقة بالجرائم الإلكترونية.	4.14	0.693	16.73%	82.81%	مرتفع
الثاني	الأمن السيبراني					
١	المؤسسة تعتمد على استراتيجيات قوية للأمن السيبراني لحماية بياناتها الحساسة.	4.11	0.724	17.64%	82.11%	مرتفع
٢	الأمن السيبراني يعد أولوية قصوى في جميع العمليات الإلكترونية	4.32	0.711	16.48%	86.32%	مرتفع

	للمؤسسة.					
٣	المؤسسة تقدم تدريبات دورية للموظفين لزيادة الوعي بالأمن السيبراني.	4.04	0.680	16.86%	80.70%	مرتفع
٤	المؤسسة مجهزة جيدًا لمواجهة التهديدات السيبرانية والتعامل مع الاختراقات الأمنية.	4.02	0.668	16.63%	80.35%	مرتفع
٥	تطبيقات الأمن السيبراني في المؤسسة تواكب أحدث التهديدات التكنولوجية.	4.01	1.017	25.36%	80.20%	مرتفع
الثالث	إدارة العمليات الإلكترونية					
١	إدارة العمليات الإلكترونية في المؤسسة تسهم في تحسين تدفق العمل وتقليل التعقيدات الإدارية.	4.23	1.001	23.67%	84.60%	مرتفع
٢	المؤسسة تعتمد على نظام إدارة عمليات إلكترونية لتنسيق ومراقبة العمليات بفعالية.	4.11	0.939	22.84%	82.20%	مرتفع
٣	إدارة العمليات الإلكترونية تقلل من الأخطاء التشغيلية وتزيد من دقة العمليات.	4.03	0.848	21.04%	80.60%	مرتفع
٤	النظام الإلكتروني لإدارة العمليات يوفر تقارير فورية تساعد في اتخاذ قرارات مدروسة.	4.00	0.802	20.05%	80.00%	مرتفع
٥	إدارة العمليات الإلكترونية تساعد المؤسسة على التكيف بسرعة مع التغيرات في السوق والطلب.	3.97	0.885	22.30%	79.40%	مرتفع
	الإجمالي للمتغير	4.11	0.7٧			

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 فأن 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 غالبًا ما يستغلون الثغرات الأمنية في أنظمة المؤسسة.	3.63	0.975	26.85%	72.63%	مرتفع
٢	معظم مرتكبي الجرائم الإلكترونية يتمتعون بمستوى عالٍ من المهارات التقنية والمعرفة الرقمية.	4.25	0.576	13.56%	84.91%	مرتفع
٣	الدوافع الرئيسية لمرتكبي الجرائم الإلكترونية تشمل الربح المالي والوصول غير المصرح به إلى المعلومات الحساسة.	4.26	0.583	13.68%	85.26%	مرتفع
٤	مرتكبو الجرائم الإلكترونية غالبًا ما يستهدفون المؤسسات ذات الدفاعات الإلكترونية الضعيفة.	4.23	0.627	14.84%	84.56%	مرتفع
٥	تتزايد قدرة مرتكبي الجرائم الإلكترونية على الابتكار وتطوير أساليب جديدة للاختراق.	4.26	0.669	15.69%	85.26%	مرتفع
الثاني	الوسيلة الإلكترونية المستخدمة					
١	مرتكبو الجرائم الإلكترونية يعتمدون على برمجيات خبيثة لاختراق أنظمة الحماية في	4.32	0.572	13.25%	86.32%	مرتفع

	المؤسسات.					
٢	التصيد الاحتيالي هو إحدى الوسائل الأكثر شيوعًا في تنفيذ الجرائم الإلكترونية.	4.42	0.596	13.48%	88.42%	مرتفع
٣	تستخدم الجرائم الإلكترونية تقنيات تشفير متقدمة لإخفاء هوية المهاجمين.	4.33	0.636	14.68%	86.67%	مرتفع
٤	الهجمات على الشبكات اللاسلكية (Wi-Fi) تُعد وسيلة شائعة لاختراق الأجهزة والأنظمة.	4.39	0.774	17.64%	87.72%	مرتفع
٥	التقنيات المتقدمة مثل الذكاء الاصطناعي تُستخدم في تطوير أدوات هجومية جديدة في الجرائم الإلكترونية.	4.32	0.760	17.60%	86.32%	مرتفع
الثالث	**الضحية**					
١	أشعر أن الوعي بالتهديدات الإلكترونية مهم جدًا لحماية نفسي من الجرائم الإلكترونية.	4.19	0.743	17.71%	83.86%	مرتفع
٢	يتأثر الجرائم الإلكترونية على ضحاياها يمكن أن يكون مدمرًا على المدى الطويل.	4.07	0.821	20.16%	81.40%	مرتفع
٣	أن الضحايا غالبًا ما يشعرون بالعزلة بعد تعرضهم للجرائم الإلكترونية.	4.23	0.780	18.44%	84.56%	مرتفع
٤	المؤسسات الأمنية تعمل جهودا كبيرا لمساعدة ضحايا الجرائم الإلكترونية كافية ومناسبة.	4.16	0.676	16.25%	83.16%	مرتفع
٥	المؤسسات الأمنية تعمل للضحايا الذين تلقوا دعمًا نفسيًا أن يتعافوا بشكل أفضل من آثار الجرائم الإلكترونية.	4.17	0.683	16.38%	83.40%	مرتفع
	الإجمالي للمتغير	4.22	٠.٧٠			

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

أولا: **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 الإحصائي
البنية التحتية التكنلوجية	0.691	0.000**
الأمن السيبراني	0.573	0.000**
إدارة العمليات الإلكترونية	0.673	0.000**
الإجمالي للمتغير (الإدارة الإلكترونية)	0.737	0.000**

المصدر: من إعداد الباحث اعتماداً على نتائج التحليل؛ (**) معنوية عند (٠.٠١) (*) معنوية عند (٠.٠٥).

نلاحظ من نتائج الجدول (٥) ان هناك ارتباط بين **الإدارة الإلكترونية وأبعادها مع الجرائم الإلكترونية** إذ بلغ معامل الارتباط للمتغير الإدارة الإلكترونية (0.737) وإبعادها **(البنية التحتية التكنلوجية والأمن السيبراني وإدارة العمليات الإلكترونية)** على توالي كلها معنوية مقارنة مستوى دلالة الإحصائية مع مستويات المعنوية (٠.٠١, ٠.٠٥) 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.

ثانيا: اختبار فرضية التأثير

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

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

الجدول (٦) نتائج تقدير العلاقة والتأثير

متغير التابع (الجرائم الإلكترونية والتكنولوجية)	الاثر						
	الارتباط	(R^2) معامل التحديد	المحسوبة (F)	الدلالة الإحصائية	Bمعامل الانحدار	المحسوبة (t)	الدلالة الإحصائية
البنية التحتية التكنلوجية	0.691	0.477	50.259	0.000	0.744	7.089	0.000
الأمن السيبراني	0.573	0.328	26.885	0.000	0.528	5.185	0.000
إدارة العمليات الإلكترونية	0.673	0.453	45.535	0.000	0.523	6.748	0.000
الإجمالي للمتغير المستقل (الإدارة الإلكترونية)	0.737	0.543	65.395	0.000**	0.670	8.087	0.000**

المصدر: من إعداد الباحث اعتماداً على نتائج التحليل؛ (**) معنوية عند (٠.٠١) (*) معنوية عند (٠.٠٥).

وكما نلاحظ من النتائج الظاهرة في الجدول (٦) ان الفرضية الرئيسية الثانية التي مفادها هناك تأثير معنوي للمتغير **الإدارة الإلكترونية و ابعادها (البنية التحتية التكنلوجية و الأمن السيبراني و إدارة العمليات الإلكترونية)** على توالي في **الجرائم الإلكترونية و التكنولوجية** قد تحققت، حيث بلغت قيمة (F) المحسوبة (65.395 و ٥٠.١٥٩، ٢٦.٨٨٥، ٤٥.٥٣٥) على التوالي وهي معنوية مقارنة بين قيمة الدلالة الإحصائية اقل من مستوى المعنوي (٠.٠٥) 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 التكنلوجية** و **الأمن السيبراني و إدارة العمليات الإلكترونية)** على توالي يفسر ما مقداره (54.3%،٤٧.٧%،٣٢.٨%،٤٥.٣%) على التوالي من التغيرات التي تحصل في العينة محل الدراسة، ونظراً على اختبار ميل الانحدار باختبار (t) و قيمة دلالة اختبار(٠.٠٠٠) وهي معنوية مقارنة بين قيمة الدلالة الإحصائية اقل من مستوى المعنوي (٠.٠٥) 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 التكنلوجية** و **الأمن السيبراني و إدارة العمليات الإلكترونية)** على توالي لها تأثيرا معنويا 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، وتُسلط الضوء على مخاطر الاختراق الإلكتروني على المؤسسات الحكومية والأمنية، وكيف يُمكن للإدارة الفعّالة أن تمنعه.

ونتيجة لهذا التحليل، توصلنا نظرياً وعملياً إلى الاستنتاجات التالية، ولهذا السبب قدمنا التوصيات

أولا: 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 كوردستان 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 تعقيدًا مع استخدام التقنيات المتقدمة مثل الذكاء الاصطناعي، ما يجعل اكتشاف الجرائم ومواجهتها أكثر تحديًا 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 أدائهم داخل المؤسسة.

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

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

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 كوردستان–العراق (٢٠٠٨). قانون رقم (٦) لسنة ٢٠٠٨: قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان–العراق، الصادر بتاريخ ١٩/٥/٢٠٠٨، منشور في جريدة وقائع كوردستان، 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 التعلمية 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.

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، آمال 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، عبود 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., Edelmann, 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.