الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ
FEDERAL AUTHORITY FOR IDENTITY, CITIZENSHIP, CUSTOMS & PORT SECURITY

أكاديمية الإمارات للهوية والجنسية
Emirates Academy of Identity and Citizenship

مجلة الإمارات للبحث العلمي

(فصلية - علمية – محكمة)

تصدر عن أكاديمية الإمارات للهوية والجنسية
مركز البحث العلمي والابتكار

الإصدار الثالث 2025

أكاديمية الإمارات
للهوية والجنسية
Emirates Academy
of Identity and Citizenship

الهيئة الاتحادية للهوية
والجنسية والجمارك وأمن المنافذ
FEDERAL AUTHORITY FOR IDENTITY,
CITIZENSHIP, CUSTOMS & PORT SECURITY

مجلة الإمارات للبحث العلمي

(فصلية - علمية – محكمة)

تصدر عن أكاديمية الإمارات للهوية والجنسية
مركز البحث العلمي والابتكار

رقم الرخصة : AD-M.L-000031

الإصدار الثالث 2025

كلمة رئيس المجلس الاستشاري لأكاديمية الامارات للهوية والجنسية:

(منصة علمية رائدة)

تواصل الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ ريادتها العلمية وجهودها المتميزة في مجال نشر المعارف والعلوم المتخصصة وتأهيل الموظفين المواطنين وتمكينهم من مواجهة التحديات المستقبلية بنجاح واقتدار، وذلك عبر ذراعها الأكاديمي أكاديمية الإمارات للهوية والجنسية

وفي هذا السياق، تصدر الأكاديمية العدد الثالث من مجلة الإمارات للبحث العلمي، التي تعد منبرًا علميًا ومعرفياً رائداً، حيث تجمع المجلة بين الأصالة والحداثة من خلال نشر دراسات وبحوث تلتزم بالمنهجية العلمية، وتواكب متطلبات التطوير المعرفي في الداخل والخارج، وتلبي متطلبات استراتيجية الهيئة ومؤشرات الأجندة الوطنية، وتوجهات دولة الإمارات العربية المتحدة، وتسهم في خدمة المجتمع وتحسين جودة حياته.

تعد المجلة بمثابة منصة علمية لتبادل الخبرات والأفكار بين الباحثين والأكاديميين، وفضاءً مفتوحاً لتلاقي الرؤى وتعميق النقاشات الفكرية في مختلف التخصصات، في ظل ما تحرص عليه إدارة تحريرها من العناية الكبيرة بتجويد ما يُنشر من أبحاث، التزامًا بمعايير النشر الأكاديمي المعتمد، وبما يضمن الارتقاء بمستوى الإنتاج العلمي محليا وإقليمياً ودولياً.

تتجسد رؤية المجلة في كونها ركيزة أساسية لدعم الابتكار والتميز، فهي لا تكتفي بكونها منصة للنشر، بل تهدف إلى خلق بيئة محفزة للبحث العلمي تسهم في معالجة التحديات الراهنة والمستقبلية. ومن خلال التركيز على المجالات ذات الأولوية الوطنية، تسعى الأكاديمية، من خلال المجلة، إلى توجيه الجهود البحثية نحو قضايا حيوية تخدم أهداف التنمية المستدامة، وتعزز من مكانة الإمارات كمركز رائد للمعرفة والابتكار

وفي هذا السياق، أشكر جميع الباحثين والمراجعين والهيئة التحريرية على ما بذلوه من جهود، راجيًا أن يحقق هذا الإصدار الإضافة العلمية المأمولة، وأن يكون لبنة جديدة في صرح المعرفة والبحث العلمي.

اللواء/ سهيل سعيد الخييلي

مدير عام الهيئة الاتحادية للهوية

والجنسية والجمارك وأمن المنافذ

رئيس المجلس الأستشاري لأكاديمية الامارات للهوية والجنسية

سياسة ومعايير النشر:

- سياسة النشر:

مجلة الإمارات للبحث العلمي هي مجلة فصلية علمية محكمة متخصصة في مجالات القانون ونظم العدالة الجنائية، والإدارة والإستراتيجية، والعلوم الاجتماعية وعلوم الأمن الوطني والأمن السيبراني والذكاء الاصطناعي. وتهدف المجلة إلى تنمية آفاق علمية جديدة لتبادل المعرفة وعرض التجارب العلمية والعملية الحديثة في المجالات التي تنسجم مع توجهات دولة الإمارات العربية المتحدة ورؤيتها وقيمها وتنسجم كذلك مع أهداف الهيئة الاتحادية للهوية والجنسية، وخدمة المجتمع الإماراتي وتعزيز الأمن والسلامة على المستوى الوطني والإقليمي والدولي. وتستهدف المجلة الأكاديميين، والباحثين ومراكز البحوث المتخصصة، والمؤسسات الحكومية ذات الصلة.

تسمح سياسة النشر في المجلة بنشر البحوث والدراسات التالية:

- البحوث التجريبية والتي تعتمد على واقع تطبيقي عملي.
- تحليل وتقييم للمفاهيم والأساليب النظرية التي يمكن تطبيقها.
- دراسات لحالات تعني بتجارب عملية واستخلاص الدروس المستفادة منها.
- دراسات مقارنات لقضايا معاصرة محلية وإقليمية ودولية.
- تحليل وتقييم لأدبيات البحث للبحوث والدارسات المعاصرة بما يفيد في تطوير وتحديث النظريات والمفاهيم في المجالات المحددة.
- تطوير نماذج وأطر نظرية جديدة تساهم في فهم أفضل للظواهر البحثية مع بيان الدلالات التطبيقية لها.
- كذلك تسمح سياسة النشر في المجلة بنشر المقالات القصيرة التي تأخذ صورة ملاحظات علمية على بحوث أو دراسات أو أوراق عمل قدمت في مؤتمرات أو ندوات علمية متخصصة أو عرض تقييمي لكتب أو ملخصات لرسائل علمية (ماجستير / دكتوراه).

- طريقة تقديم البحوث والمقالات للنشر:

تقبل البحوث والدراسات المقدمة باللغات العربية والإنجليزية فقط وترسل إلى البريد الإلكتروني RecearchCenter@icp.gov.ae باسم رئيس تحرير مجلة الإمارات للبحث العلمي». ويرفق مع البحث إقرار موقع من المؤلف بأن البحث المقدم للنشر لم يُنشر من قبل وأنه لن يقدم لأي جهة حتى تنتهي إجراءات التحكيم.

- الاشتراطات الشكلية للنشر:

ينبغي على المؤلف التزام بالشروط الشكلية التالية قبل تقديم البحث:

أن يحتوي البحث على:

- صفحة غلاف تتضمن عنوان البحث، واسم المؤلف، ووظيفته، والمؤسسة التي يعمل فيها، وعنوانه ورقم هاتفه والبريد الإلكتروني باللغتين العربية والإنجليزية.
- ملخص البحث على ألا يتجاوز 250 كلمة باللغتين العربية والإنجليزية
- مقدمة البحث
- مشكلة الدراسة وتساؤلاتها
- أهمية الدراسة
- أهداف الدراسة
- فرضيات الدراسة (إن وجدت)
- الإطار النظري والدراسات السابقة
- منهجية الدراسة
- مجتمع الدراسة وعينتها
- تحليل البيانات واختبار الفرضيات
- النتائج والتوصيات
- الملاحق (إن وجدت)
- قائمة المراجع

1. ألا تتجاوز عدد صفحات البحث 100 صفحة ولا تقل عن 50 صفحة بما في ذلك المراجع والملاحق.
2. مواصفات الطباعة: نوع الخط (Times New Roman)، حجم الخط 14، الهوامش 4 سم في أعلى وأسفل وعلى جانبي الصفحة.
3. الجداول والصور: تأخذ كل الجداول والصور أرقاما متسلسلة تدرج أسفل الجدول/الصورة مع رقم الجدول/الصورة والاسم والمصدر.
4. المراجع في المتن يشار إلى جميع المراجع في متن البحث مع ضرورة الإشارة إلى الاسم الأخير للمؤلف (العائلة) وسنة النشر بين قوسين الكندي، 2025).
5. قائمة المراجع: تدرج قائمة للمراجع في نهاية البحث مرتبة هجائي حسب أسم المؤلف مع ضرورة استكمال كل البيانات الببليوجرافية لكل مصدر.

- تحكيم البحوث والمقالات المقدمة للنشر

يتم تحكيم البحوث والدراسات وفقاً للمعايير الأكاديمية المعروفة وبموجب نماذج للتحكيم

والتقييم المعتمدة في الأكاديمية. ومن أهم المعايير المستخدمة في تقييم البحوث والدراسات التحقق من مدى أصالتها والإسهام الذي تقدمه من ناحية علمية وعملية. ويتم التحكيم من أستاذة متخصصين ممن لهم رصيد متميز من الإنتاج والبحث والعلمي. وتخضع البحوث المقدمة للنشر للإجراءات التالية:

1. فحص أولي يجريه أعضاء هيئة التحرير.
2. تقييم سري يجريه ثلاثة محكمين للبحوث التي اجتازت الفحص الأولي.
3. تقرير صلاحية البحوث والدراسات المقدمة للنشر بواسطة المحكمين.
4. إرسال تقرير المحكمين للمؤلف يحتوي على نتيجة التحكيم وقرار هيئة التحرير خلال مدة أقصاها 3 أشهر من تاريخ تسليم البحث.
5. في حالة قبول نشر البحث، يتم إخطار المؤلف بالنشر وتاريخه.

حقوق النشر

محتويات الإصدار الثالث:	
The Impact of AI-Driven Decision Support Systems (DSS) in Border Authorities. د. محمد خميس مسعود الشامسي	1
التفريد القضائي وأثره في تحقيق مقصد الشارع من العقاب. د. محمد إسحاق الخاجه	2
استدامة ريادة الخدمات: دراسة تطبيقية على الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ في دولة الإمارات د. سعيـد أحمـد سودين البلوشـي	3
التهديدات السيبرانية الناشئة للخدمات الرقمية بالهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ وطرق التعامل معها الباحث / عبدالرحيم علي محمد عبدالرحيم الانصاري	4

الفهرس

بحث بعنوان:

The Impact of AI-Driven Decision Support Systems (DSS) in Border Authorities.

تأثير أنظمة دعم القرار المعتمدة على الذكاء الاصطناعي في سلطات الحدود بالهيئة

د. محمد خميس مسعود معيوف الشامسي
أستاذ إدارة التكنولوجيا
أكاديمية الإمارات للهوية والجنسية

Abstract

Objective: The present study examines how system design (SD) and organizational support (OS) impact the perceived ease of use (PEU) and the adoption of artificial intelligence (AI) technologies within organizations with special reference to border authorities.

Methods: A survey that was cross-sectional was conducted online to 209 participants via Google Forms. The survey comprised validated Likert-scale items designed to measure the study's constructs. Furthermore, a questionnaire included in the study was taken from previous studies. Data were examined using SPSS for both descriptive and SmartPLS 4 for structural equation modeling in order to assess the formulated hypotheses.

Results: The investigation verified that system design (SD) has a statistically significant effect on perceived ease of use (PEU) ($\beta = 0.727$, $p < .001$) and that PEU positively influences AI adoption (AI) ($\beta = 0.788$, $p < .001$). However, organizational support (OS) did not demonstrate an important impact on PEU ($\beta = 0.073$, $p = .434$), which suggests its limited role in affecting user perceptions of ease of use directly.

Keywords: Artificial Intelligence; Organizational Support; Perceived Ease of Use; System Design; Technology Adoption

Introduction

1.1 Background of the Study

Making computers behave like humans is the concept of artificial intelligence (AI); therefore, a lot of AI technology is widely used in business (Pelau, Dabija & Ene, 2021). For example, the United States artificial intelligence business was projected at USD 42.00 billion in 2023, and the country has achieved significant advances in AI and robotics. Moreover, the European business of artificial intelligence is anticipated to expand at a significant CAGR of 33.2% between 2024 and 2030. The finance industry in Europe is undertaking considerable transition as AI technologies become more widely adopted. Ad-

worldwide revenue. AI is used by schools and colleges in the Asia Pacific region to help students do better by implementing personalized learning experiences, data analysis, and smart teaching systems. Finally, by 2030, the region of the Middle East and Africa's (MEA) AI market is expected to grow to a value of USD 166.33 billion. The expansion of the AI sector in Saudi Arabia, which is part of the Middle East, is fueled by a variety of initiatives, laws, and financial assistance schemes. The Authority for Saudi Data and AI (SDAIA), for example, is a government organization that develops an AI ecosystem involving both public and commercial sector organizations. Creative AI-based solutions are implemented by SDAIA, including methods for fusing data and AI in important domains (AI Market, 2021). Moreover, aligned with the UAE Centennial 2071, the UAE aims to become a leader in AI by 2031, opening up new economic, social, and educational opportunities for corporations, governments, and individuals alike, and producing an additional AED 335 billion in growth. In the UAE, using AI-powered decision-support tools are growing in order to enhance the ability to make decisions in many industries. The UAE has acknowledged the value of artificial intelligence (AI) in project management, with studies highlighting the incorporation of AI at every stage of the project to optimize workflows and guarantee more informed choices (Al-Obeidi, 2022). Furthermore, studies have shown that both internal and external factors can help people adopt new technologies. One example is how technology and employee influence helped the UAE's government successfully implement AI-driven e-innovation projects (Aliakbar et al., 2022). AI-driven Decision Support Systems (DSS) are crucial to border authorities due to its advanced tools and methods to support human decision-makers, fostering a cooperative relationship between people and AI models. In this study, the researcher wants to look into what influences the use of AI-driven Decision Support Systems (DSS) in UAE Border Authorities

1.2 Problem Statement

On Tuesday, April 9, 2024, as stated by Paul Griffiths, CEO of Dubai Airports,

around 2,155 flights were cancelled, marking the highest quantity of cancellations to date. Approximately 75,000 meals were provided to travelers at Dubai International Airport and Dubai World Central (Salim, 2024). Moreover, according to the Guardian, Dubai received more than 142 mm of rain, setting a record for an 18-month period. As a result, border officials are increasingly contemplating the use of AI-driven decision support systems (DSS) to improve real-time traffic management and emergency preparation during severe rains. Nevertheless, the effective implementation of such technologies are dependent on knowing the elements that impact the use of the systems among border officials

1.3 Research Questions

RQ 1) How does system design influence the perceived ease of use of AI technologies?

RQ 2) Does organizational support enhance the perceived ease of use of AI technologies?

RQ 3) How does perceived ease of use affect the adoption of AI technologies in organizations

1.4 Research Objectives

The purpose of the study is to look into the factors that impact the use of AI-driven DSS in border officials of the United Arab Emirates.

Facilitate the analysis of the link between these elements and the constructs of TAM (Technology Acceptance Model).

1.5 Significance of the Study

- This study enables the creation of an environment for management review and understand the true effect of this system on improving administrative performance.
- A few border officials have made the deployment of AI-driven DSS a top priority in recent years because of the significance and advancements in artificial intelligence and database management. The process of collecting, ana-

lyzing, and storing data is the main focus of this area (Azeez & Yaakub, 2019).

- Improving collaboration between immigration authorities, government entities, and international groups because of its versatility, continuous learning capabilities, and user-friendly interfaces.
- Improving decision-making is directly positively correlated with individual productivity, organizational culture, and organizational performance, according to the study.
- Effective border control operations depend on the cooperation of human decision-makers and AI models in decision support systems.

1.6 Terminology of the Study

- Artificial intelligence (AI): making computers behave like humans is the concept of artificial intelligence (AI), and as a result, a lot of AI technology is widely used in business (Pelau, Dabija & Ene, 2021).
- AI-driven Decision Support Systems (DSS): increase effectiveness and efficiency of border administration by evaluating enormous volumes of data (Kokkalis et al., 2020).
- Border authorities are managers, supervisors, and border control officials of the Federal Authority for Identity, Citizenship, Customs, and Port Security.

1.7 Delimitation of the Study

Delimitation establishes the study's boundaries and scope. This section ensures clarity and manageability within the research framework by defining the study's focus and exclusions. The first one is geographic scope; the investigation will be carried out inside UAE border authorities. It will cover the three main categories of border checkpoints: land borders, ports, and airports. Managers, supervisors, and border control officials are among the participants. Furthermore, system scope refers to AI-driven decision support systems that border authorities will use in the future, and it is the main focus of the study. Additionally, numerous aspects of these systems, such as utility, design, functioning, and ease of use, will be investigated in this study.

As a final point, the theoretical scope will examine constructs including perceived usefulness, system design, behavioral intention to use the system, and perceived ease to use, all under the guidance of the Technology Acceptance Model (TAM). These boundaries are intended to keep the research relevant, controllable, and well-defined, while also offering targeted and practical insights into the adoption and application of AI-driven decision support systems within border authority

1.8 Limitation of the Study

There is a chance that the sample does not accurately reflect all global border agencies. Because different locations have different operating contexts, policies, and technological breakthroughs, the conclusions drawn from one region or nation may not apply to others. Even though a large number of participants can provide detailed information through surveys, qualitative techniques like focus groups and interviews may be able to provide deeper insights. Because technology, regulations, and user experiences are always changing, the study's observations and actions may not accurately reflect changes over time. Some potential participants may also be hesitant to participate in the study due to concerns about data protection. At last, the study can yield significant insights by being honest about its limits and potential biases

2 Literature Review and Previous Studies

In this particular passage, the researcher is reviewing studies that are related to the study. A literature review discusses conflicts, gaps, issues, and unsolved problems in past studies while also providing a foundation of knowledge in the field.

2.1 Artificial Intelligence (AI)

Nowadays, there are a lot of solutions that artificial intelligence offers. For instance, Islam et al. (2022) disclose that explainable artificial intelligence (XAI) has grown significantly; its models are quite accurate, but they are not interpretable or explainable. A systematic literature assessment of 137 publications reveals that AI techniques, designed primarily for applications where safety is crucial, more frequently utilize group models and deep learning.

End users are more likely to accept visual explanations, and strong assessment metrics are being created to rate the effectiveness of explanations. Developing explanations for broad users from delicate sectors like finance and the legal system requires more focus. Moreover, from 1970 to 2020, Bozkurt et al. (2021) employed three research clusters of AI studies in education: technological, pedagogical, and artificial intelligence. The document proposes five overarching study themes: AI in higher education, AI-generated data utilization, educational human-AI interaction, deep learning, and adaptive learning. It also emphasizes how crucial ethics are to AI research. Additionally, Gökalp et al. (2024) use artificial intelligence and the process of the analytic hierarchy (AHP) to examine the significance of public health improvement methods. To generate the decision matrix, a spherical fuzzy sets framework is used, allowing experts with higher qualifications to take it into account. According to the finding's, improving accessibility is the most important strategy to enhancing the health of its public, but immunization as well as preventative programs are also quite essential. This strategy guarantees a longer and better life while assisting policymakers in addressing time and financial constraints. Furthermore, Chiu et al. (2024) seek to define AI proficiency and knowledge in K–12 classrooms by incorporating self-assurance and self-analysis. This study suggests a thorough structure for teaching artificial intelligence that emphasizes technology, impact, ethics, teamwork, and awareness. The five main elements of the framework are self-reflection, technology, ethics, impact, and collaboration. The study also outlines five learning activities that are beneficial in building skills and self-assurance. The next areas of research to be undertaken include empirical research, self-reflective thinking, algorithmic literacy, data literacy, prompt engineering, and reflective mindset. Contrarily, three dependent variables which are organizational performance, individual productivity, and organizational culture, were highlighted by Alasmri et al. (2022). Their investigation explores how artificial intelligence (AI) affects decision-making in Saudi businesses. Enhancing

decision-making was directly positively correlated with individual productivity, organizational culture, and organizational performance, according to the findings. In order to better prepare managers for AI and enhance their decision-making procedures, the study offers implications and recommendations. Likewise, Kerimovs (2024) offers an AI model that uses a variety of data sources to forecast the locations of unlawful border crossings. The methodology offers real-time risk evaluations, outperforming conventional techniques in terms of effectiveness and affordability. It is relevant in tackling border security concerns and improving cooperation between international organizations, government agencies, and immigration agencies because of its versatility, continuous learning capabilities, and user-friendly interfaces. A number of studies were done to investigate how AI affected the UAE government's decision-making process (Bejger & Elster, 2020; El Emary, Al Otaibi & Al Amri, 2020; Stone et al., 2020). The study discovered a strong correlation between higher transaction efficiency, lower costs, and better service quality when employing AI. Knowing the elements that affect the utilization of the AI model among border officials is one of the goals in this study. Therefore, the next section is about the adoption of AI-driven DSS.

2.2 Adoption of AI-driven DSS

AI-driven Decision Support Systems (DSS), which integrate human knowledge and AI expertise, are essential to border authorities. Machine learning models are employed to perform data analysis, simulate human cognitive functions, and mitigate biases. AI-powered cameras used in border security show how it may improve security and control (Sanja, 2022; Karolina et al. 2022; Forster, 2023; Kacprzyk, 2022). Other authors defined AI-driven DSS as an assessment of flood risk management during heavy rainfall events. The system works by combining different types of data, like weather forecasts, historical flood data, and hydrological models, to give real-time assessments of the risk of flooding and suggestions for what to do (Smith & Johnson,

2020; Chen & Zhang, 2019; Li & Wang, 2018). Furthermore, according to Kokkalis et al. (2020), AI-powered DSS increase the accuracy and efficiency of border administration by evaluating enormous volumes of data from travel documents, ad hoc border checks, and databases. These systems are capable of automating asylum application responses, predicting criminal threats, and doing risk evaluations. Artificial intelligence (AI) technology, such as biometrics, UAVs, thermal cameras, lie detectors, and e-gates, simplifies procedures and gives European border services a full toolkit to protect their external borders against irregular migration and transnational criminal activity. Likewise, as stated by Hung (2012) the adoption of AI-powered DSS varies by industry and is affected by several factors. These factors contain compatibility, perceived behavioral control, attitude, subjective norms, perceived ease of use, and perceived usefulness. Furthermore, studies on the adoption of CDSS underlines the significance of elements such as effort expectancy, facilitating conditions, task technology fit, technology characteristics or system design, performance expectancy, and task characteristics in determining general practitioners' acceptance of CDSS (Aljarboa et al., 2019; Aljarboa et al., 2020). Panicker et al. (2023) also say that how useful people think AI-driven Decision Support Systems (CDSS) are is a big factor in how many people use them. Finally, effective border control operations depend on the cooperation of human decision-makers and AI models in decision support systems, highlighting the significance of this partnership to optimize real-time traffic management and emergency preparation during severe rains (Tosin et al., 2023). Similarly, Alamanos et al. (2021) have underlined the significance of integrating organizational support interaction and analysis within the DSS framework as a critical component of readiness. Border authorities may ensure that the DSS meets their objectives and priorities by incorporating stakeholders in its development and implementation. This will increase the system's acceptance and utilization rates Karen et al. (2016) have created a decision support toolkit to facilitate multi-agency de-

cision-making in cross-border emergencies. This toolkit enables quick and efficient handling of all phases in the lifespan of emergency management, including response, recovery, preparedness, and mitigation. A comprehensive framework for healthcare readiness, response, and recovery is proposed by the project, which incorporates rapid development, responder training, risk sharing, interoperability standards, healthcare spatial data management, and simulation preparation for system analysis. User perceptions heavily influence the acceptability of AI technology, whereas trust is determined by experiences and degree of trust. User intention is impacted by elements like as innovation, usefulness, ease of use, quality of information, and personalization all influence user intention. In order to ensure a beneficial influence on individuals and society, it is imperative that organizations deploying AI understand and address these misunderstandings (Yi & Choi, 2023; Liehner et al., 2023; Choudhury et al., 2023; Goli et al., 2023). Moreover, Bokhari & Myeong (2023) and Ho et al. (2022) indicated that cultural factors are influencing the adoption of AI-driven DSS. In addition, when AI tools are integrated, trends may be continuously monitored, which improves detection accuracy over time, lowers false positive rates, and increases the identification of real security threats (Sherry Bor & Nicole Koech, 2023). Understanding the factors that impact the use of AI-driven decision support systems is essential for humans to successfully implement and use them in a variety of industries. Next, the researcher discloses the use of TAM, which is the Technology Acceptance Model

2.3 Technology Acceptance Model

The Technology Acceptance Model is the most widely used paradigm for characterizing user acceptance behavior, developed by Davis in 1986. It is founded on the principles of rational action and social psychology theory, which claim that beliefs impact attitudes and usage intents. In the years 1989-2001, there were approximately one hundred TAM-related researches that were published in technology-related publications, conferences, or

reports. Drawing on varying sample sizes and internal/external user groups between enterprises, TAM was thoroughly evaluated in these studies, analyzed to draw meaningful conclusions contrasted with rival theories (Gefen et al., 2000). Many end-user technologies were employed with it, such as word processors (Davis et al., 1989; Taylor & Todd, 1995b); spreadsheets (Agarwal et al., 2000; Mathieson, 1991); email (Adams et al., 1992; Davis, 1989); and the World Wide Web (Lederer et al., 2000). Additionally, one important component of the Technology Acceptance Model (TAM) for AI-driven decision support systems (DSS) is the impact of system design on perceived usefulness (Venkatesh et al., 2003). TAM has also been extended in a number of studies by adding elements such as self-efficacy, gender, experience, and culture. Generally, studies indicate that TAM is strong, valid, and thrifty Venkatesh & Davis, 2000

.3 Methodology

3.1 Approach of the Study

The researcher makes use of a quantitative method, specifically a cross-sectional survey methodology that employs structured questionnaires to collect information from border authority staff regarding their opinions and encounters with the AI-driven DSS.

3.2 Proposed Model

According to the literature reviews, the proposed model's four main constructs are essential elements. Perceived ease of use, for example, reveals user interface, training, support, and integration. On the other hand, the study's outside factors are system design, which explained both customization and reliability, as well as organizational support, which contained both management support and resource allocation. Finally, the dependent variable represents the attitude towards the usage of AI-DSS. Figure 1 below depicts the proposed research model

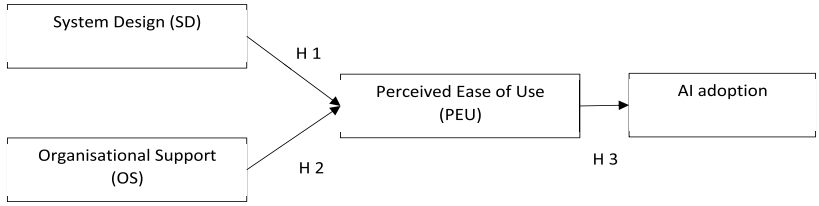


Figure.1. Proposed Model of the research (Designed by author)

3.3 Participants of the study

These participants are randomly selected through the use of a systematic method, with the target population for the study consisting of border authority personnel who work at several types of checkpoints, such as land borders, seaports, and airports, and who will be the main users of AI- DSS. Table 1 presents the demographic characteristics of the sample (N = 209) with a clear representation of gender, work experience, professional status, and workplace location

(Table 1. Demographic data (N= 209)

Variables	Values	n	%
Gender	Male	165	78.9%
	Female	44	21.1%
Work Experience	Less than 5 years	8	3.8%
	to 10 years 5	29	13.9%
	Above 10 years	172	82.3%

Professional status	Leadership (Director/Deputy Director/Office Director/ Department or Branch Manager/ (Administrator	80	38.3%
	Officer (inspection, analysis, targeting, evaluation)	86	41.1%
	Support Officer (Technical/Administrative)	43	20.6%
Workplace	Air ports	66	31.6%
	Sea ports	30	14.4%
	Land ports	17	8.1%
	Affiliated to the Authority›s main headquarters	96	45.9%

The majority of participants were males (78.9%), with females comprising 21.1% of the sample, which means a male-dominated group. Most participants had extensive work experience, with 82.3% having more than 10 years in the field, which reflects a well-established and knowledgeable workforce. Professionally, the sample was diverse: 41.1% were officers involved in inspection, analysis, targeting, and evaluation; 38.3% held leadership roles such as directors and managers; and 20.6% were support officers in tech-

nical or administrative positions. Regarding workplace location, nearly half of the participants (45.9%) were affiliated with the authority's main headquarters, followed by 31.6% based at airports, and smaller proportions at seaports (14.4%) and land ports (8.1%

3.4 Tools of the Study

The questionnaire is the study's tool for gathering data from participants. The questionnaire comprises two parts, with the first section dedicated to collecting demographic data, whereas the second section consists of 5 points on the Likert scale items related to the study's constructs. Lastly, a questionnaire included in the study was taken from previous studies and translated to Arabic as shown in

3.4.1 Validity and Reliability of the Study

The researcher verified the study tool's validity by presenting the questionnaire to a committee of professionals specializing in border security. The degree to which the study tool yields consistent results was verified through the execution of a pilot study with 11 specialists and calculating Cronbach's alpha values for the questionnaire as a whole, which was 0.85, which is higher than the cutoff point of 0.70 (Hair et al., 2023)

3.4.1 Data Collection Procedure and Distribution

Using survey software such as Google Forms, the researcher has created an electronic copy of the survey. Then, the investigator sent out the questionnaire through email and the border authority' internal communication channels. The questionnaire includes a cover note outlining the goal of the research, guaranteeing anonymity and confidentiality, and giving directions on how to fill out the survey. To encourage involvement, the researcher has sent out follow-up emails and reminders. Finally, to guarantee enough time for responses, the given time period was four weeks to collect data

4.1 Data Analysis

Testing the research questions and extracting valuable insights from the gathered data. The following outlines the precise strategy for examining the information gathered via the survey

4.2 Data Preparation

The initial phase is data cleansing, in which the determination of missing data and how to address them is made. Furthermore, the detection and management of outliers, as well as ensuring that all responses fall within the expected range. Finally, converting demographic information into numerical codes for analysis

4.3 Statistics

SPSS and SmartPLS 4 were used for data analysis. For preliminary analyses, SPSS was used, which included descriptive statistics and data cleaning. SmartPLS 4 was used for the main analysis, which included assessing the measurement model and testing the structural model through path analysis. The bootstrapping technique in SmartPLS 4 was used to test the hypotheses and generate t-values, p-values, and beta coefficients for the path coefficient

4.4 Measurement Model

In order to assess important quality indicators like convergent validity, discriminant validity, and other external model indicators, this study uses outer loadings, average variance extracted (AVE), and composite reliability (CR), in accordance with the analysis and evaluation framework proposed by Hair et al. (2020). As per the criteria presented by Ramayah et al. (2018), loadings AVE and CR have threshold values of 0.7, 0.5, and 0.7, respectively. According to the data presented in Table 2, all item loadings exceeded the 0.7 threshold, indicating strong item reliability. The AVE values for all constructs were greater than 0.5, ensuring adequate convergent validity, and the CR values exceeded 0.7, confirming the constructs' internal consistency and reliability. This suggests that the measurement model adequately captures

the variance attributed to the constructs compared to the variance caused by measurement error. Further examination of discriminant validity was conducted using the heterotrait-monotrait (HTMT) ratio as proposed by Franke and Sarstedt (2019). An HTMT value less than 0.90 suggests that the constructs are sufficiently distinct, which confirms discriminant validity. The HTMT ratios, detailed in Appendix B, mostly fell below the 0.90 threshold. Subsequent HTMT bootstrapping results indicated that the upper limits (UL) between variables over the proposed threshold were less than 1.0. This outcome supports the notion that respondents perceived the two main predictor constructs tested as independent, which further validates the discriminant integrity of the model.

Table 2. Measurement Model Loadings, AVE, and CR

Construct	Item	Loading	AVE	CR
AI Adoption (AI)	BIU1	0.904	0.84	0.92
	BIU2	0.916		
	BIU3	0.922		
	BIU4	0.872		
Organizational Support (OS)	OS1	0.933	0.87	0.95
	OS2	0.93		
	OS3	0.916		
	OS4	0.897		

Perceived Ease of Use (PEU)	PEU1	0.942	0.88	0.94
	PEU2	0.943		
	PEU3	0.871		
	PEU4	0.869	0.85	0.93
System Design (SD)	SD1	0.844		
	SD2	0.891		
	SD3	0.837		
	SD4	0.912		

4.5 Structural Model

To verify the suggested hypotheses about the relationships inside an AI adoption framework, this study used 5,000 bootstrap resamples to conduct a structural model analysis (Hair et al., 2020; Ramayah et al., 2018). The bootstrap analysis yielded confidence intervals, t-values, p-values, beta coefficients, and standard errors, which provides a robust examination of the paths within the model

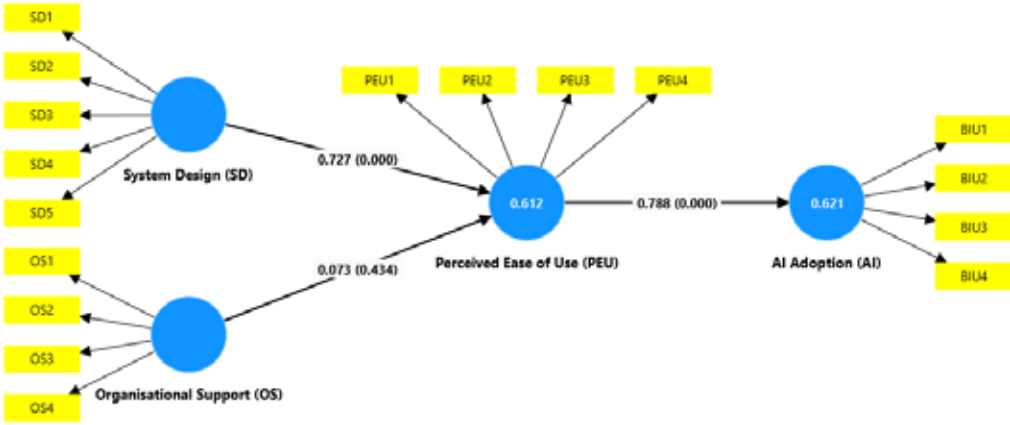


Figure 1. Hypothesis Testing Results (SmartPLS 4)

System Design (SD) significantly influences Perceived Ease of Use (PEU) with a beta coefficient of β = 0.734, t = 9.980, p <.001, showing a substantial and statistically significant effect. The organizational support (OS) to perceived

ease of use (PEU) relationship was weaker and not statistically significant with a beta coefficient of β = 0.120, t = 1.388, p =.165. A strong relationship was observed from perceived ease of use (PEU) to AI adoption (AI) with a beta coefficient of β = 0.820, t = 23.641, p <.001, which means a significant positive effect. The analysis also explored the total effects, revealing that system design (SD) through perceived ease of use (PEU) strongly predicts AI adoption (AI), as evidenced by a beta of β = 0.601, t = 9.261, p <.001. The indirect effect of organizational support (OS) through perceived ease of use (PEU) on AI adoption was minimal and not significant (β = 0.099, t = 1.370, p =.171).

These findings confirm that the ease of use of AI systems, significantly influenced by system design, plays a critical role in their adoption, whereas organizational support, though positive, does not show a significant direct effect in enhancing the perceived ease of use or adoption of AI systems. This aligns with the theoretical framework posited by prior research, underscoring the pivotal role of user-perceived system characteristics in technology adoption processes. In short, research questions RQ1 and RQ3 are supported, which means that both system design and perceived ease of use are critical to AI adoption. The research question RQ2 is not supported, indicating that organizational support alone may not have a significant impact on perceived ease of use within the context studied. These outcomes contribute valuable insights to the body of knowledge on technology adoption, particularly in the context of AI systems.

5. Discussion

This section of the study evaluates the influence of system design, organizational support, and perceived ease of use on AI adoption. This analysis is enclosed inside the framework of the Technology Acceptance Model (TAM), which posits that system design and organizational support are pivotal in shaping users' perceptions of technology ease of use and their subsequent adoption decisions (Davis, 1989). Research question 1: System design (SD)

positively influences perceived ease of use (PEU). The first research question is about whether an effective system design enhances the perceived ease of use. The data supports this claim (β = 0.727, p <.001), which suggests a strong positive relationship between system design and perceived ease of use. This result is consistent with previous studies that found that user-friendly and intuitive design features can significantly enhance users' technology engagement by reducing complexity and improving usability (Venkatesh & Bala, 2008). Such designs are crucial as they can diminish the cognitive load on users, therefore raising the possibility that technology will be adopted (Zhang, 2007). Research question 2: Organizational support (OS) positively influences perceived ease of use (PEU). The second research question examined the role of organizational support in enhancing the perceived ease of use. While the path coefficient was relatively small (β = 0.073), it was not statistically significant (p =.434). Consequently, it implies that organizational support alone may not be a strong predictor of perceived ease of use. This finding aligns with the notion that while support mechanisms such as training and user assistance are important, they might not directly influence users' immediate perceptions of ease of use unless they are specifically targeted at mitigating usage complexities (DeLone & McLean, 2003). It suggests that other factors, such as personal user experience and system quality, may play a greater role in influencing perceived ease of use. Research question 3: Perceived ease of use (PEU) positively influences AI adoption (AI). The third research question is about whether the perceived ease of use would positively influence AI adoption. This research question found support in the data (β = 0.788, p <.001), underscoring that ease of use is a critical determinant of AI technology adoption. This result is in harmony with TAM, where ease of use is considered, a fundamental factor influencing the acceptance and utilization of new technologies (Davis, 1989). The finding suggests that when users perceive a technology as easy to use, they are more likely to adopt it. This is

particularly relevant in the context of AI technologies, where the perceived complexity can often be a barrier to adoption (Lee & Lee, 2020).

The study's findings provide substantial support for the critical roles of system design and perceived ease of use in the adoption of AI technologies. While organizational support did not have a significant direct effect on perceived ease of use, it may still be considered essential in a broader support context, particularly when aligned with specific user needs. These insights contribute to the existing literature on technology acceptance and offer practical implications for organizations aiming to enhance AI technology adoption among their users

5.1 Implications

The findings of this investigation have multiple practical implications for organizations and IT developers focusing on AI technology adoption. First, the strong influence of system design on perceived ease of use suggests that developers should prioritize user-friendly and intuitive interfaces to facilitate adoption. These design features can significantly enhance user engagement by reducing complexity and improving usability, thereby increasing the likelihood of technology acceptance (Venkatesh & Bala, 2008). Furthermore, although organizational support did not have a significant impact on perceived ease of use, it remains critical in providing the necessary resources and training for users. Organizations should consider aligning their support mechanisms more closely with specific user needs to effectively enhance the adoption process DeLone & McLean, 2003

5.2 Limitations

There are several limitations on this study. First, the sample was limited to professionals from specific port authorities, which could restrict how broadly the results can be applied to other sectors or contexts. Second, it is difficult to establish causal relationships from the data because of the study's cross-sectional nature. Longitudinal studies might deliver more insight into how perceptions and adoption intentions change across time. Furthermore,

using self-reported metrics could result in response biases, which could influencing the accuracy of the data collected.

5.3 Recommendations and Suggestions for Future Research

Several recommendations for additional study can be made in view of the limitations and results of the current study. To improve the generalizability of the results, future research could broaden the sample to cover a wider range of sectors and geographical areas. To obtain a more thorough understanding of AI technology adoption process, longitudinal study methods can be used to track changes in attitudes and adoption patterns over time. Furthermore, using qualitative techniques like focus groups and interviews could yield more detailed information on user opinions and experiences, leading to a more complex understanding of the variables affecting the adoption of AI. Future research could examine other variables that could affect the adoption of AI technologies, such as individual characteristics (like technology readiness) or external factors like ethical and regulatory considerations related to AI use, in an effort to further refine the model used in this study. These elements may offer a more thorough understanding of the landscape of technology adoption and aid in the creation of more focused interventions to raise adoption rates

5.2 Conclusions

In conclusions, the limits of the study indicate that future research should employ qualitative techniques like focus groups and interviews to understand user viewpoints and experiences, use longitudinal methods to track trends in AI adoption, and broaden the sample to encompass a greater range of sectors and geographic areas. Furthermore, examining personal traits as well as outside variables like moral and legal issues may offer a more thorough comprehension of technology adoption. Effective system design is crucial in enhancing user engagement and facilitating the adoption of AI technologies. The findings suggest that while organizational support is beneficial, its im-

pact on PEU is less direct and may depend on other mediating factors. This research adds to our understanding of technology acceptance models and has applications for IT governance and the thoughtful application of AI in corporate environments.

6. Practical Research

6.1Input

Real-Time Data Integration and Management Data Collection, data storage, and data Preprocessing.

Predictive and Prescriptive Analytics Predictive Modeling, risk assessment, and Scenario Analysis.

Machine Learning and AI Models Anomaly detection, classification models, Sentiment Analysis.

Natural Language Processing (NLP)Text mining, language translation, automated Summarization.

Geospatial Analysis and VisualizationMapping and visualization, geofencing, Heatmaps.

Communication and Collaboration Tools Alert systems, collaboration platforms, incident Management

Decision Support and Automation Decision trees, automated workflows, Resource Allocation.Reporting and Documentation

Real-time dashboards, automated reporting, Audit Trails.

Security and Compliance

Access control, data encryption, compliance Monitoring.Post-Crisis Analysis and Learning

After-action reviews, knowledge management, continuous improvement.

6.2 Processing

Initiation Phase Define Objectives, feasibility study, stakeholder identification: Identify all sponsoring organizations, technical teams, and end users are examples of stakeholders. Make certain their needs and expectations

are well understood. Planning Phase Project plan development, risk management, resource allocation, data collection and preparation. Execution Phase System Design and Development, integration, training and testing, end users should receive
training so they can operate the system efficiently. This includes training on how to interpret AI-generated insights and make decisions based on them Monitoring and Control Phase Progress Tracking, quality assurance, performance evaluation, issue Resolution: Address any issues or challenges that arise during the project. This includes technical issues, stakeholder concerns, and resource constraints Closure Phase Final Testing and Validation, documentation, feedback collection: find out what needs to be improved by getting input from end users and stakeholders. Use this feedback to make necessary adjustments and enhancements.Project Review: Conduct a project review to assess the success of the project. Identify lessons learned and best practices that can be applied to future projects.Post-Implementation Support Maintenance and Support, performance monitoring, and project review

6.3Output

Predictive Analytics and Forecasts Future Trends, and risk Assessment: Identifying potential risks and their likelihood, which helps organizations prepare and mitigate these risks in advance.Real-Time Alerts and NotificationsEmergency Alerts, and operational Alerts: Updates on system performance, deviations from expected performance.Optimization Recommendations Resource Allocation and process improvement: Recommendations on improving existing processes or workflows based on data analysis. Visualizations and Dashboards Interactive Dashboards, and heatmaps and geospatial Analysis: Visual tools that highlight critical areas or hotspots, useful in various applications like disaster response or supply chain management. Decision Recommendations

Strategic Decisions, and tactical decisions:
Specific, actionable recommendations for immediate implementation, often with suggested actions and possible outcomes. Scenario Analysis What-If Scenarios, and simulations: Running
simulations to visualize outcomes of various strategies, which aids in preparing for future events Knowledge Extraction and Insights Patterns and Trends: Identifying and highlighting significant patterns and trends from large datasets. Sentiment Analysis: Understanding public sentiment or stakeholder opinions from textual data sources like social media or survey responses.

References:

Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived usefulness, ease of use, and usage of information technology: A replication. MIS quarterly, 227-247.

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). The evolving relationship between general and specific computer self-efficacy—An empirical assessment. Information systems research, 11(4), 418-430.

Alasmri, N., & Basahel, S. (2022). Linking artificial intelligence use to improved decision-making, individual and organizational outcomes. International Business Research, 15(10).

Aliakbar, Al-Obeidi., Muaath, S., Al-Mulla. (2022). The Legal Basis of the Right to Explanation for Artificial Intelligence Decisions in UAE Law. 1-4. doi: 10.1109/ACIT57182.2022.9994088 A. Alamanos, A. Rolston, & G. Papaioannou. (2021). Development of a Decision Support System for Sustainable Environmental Management

Aljarboa, S., & Miah, S. J. (2019, December). Investigating acceptance factors of Clinical Decision Support Systems in a developing country context. In 2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE) (pp. 1-8). IEEE.

Aljarboa, S., & Miah, S. J. (2020, December). Assessing the acceptance of clinical decision support tools using an integrated technology acceptance model. In 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE) (pp. 1-6). IEEE.

Al-Obeidi, A. H., & Al-Mulla, M. S. (2022, November). The Legal Basis of the Right to Explanation for Artificial Intelligence Decisions in UAE Law. In 2022 International Arab Conference on Information Technology (ACIT) (pp. 1-4). IEEE.

Artificial Intelligence Market Opportunities, Type & Forecast 2028. (2021b, November 1). Data Bridge Market Research, https://www.databridge-marketresearch.com, All right reserved 2024. https://www.databridge-marketresearch.com/reports/global-artificial-intelligence-market

Azeez, R. T., and Yaakub, K. B. (2019). The Relationship between Management Information Systems and Total Quality Management: A Survey Study at Missan Oil Company in Iraq. International Journal of Business and Social Science, 10(2).

Bagozzi, R. P., Davis, F. D., & Warshaw, P. R. (1992). Development and test of a theory of technological learning and usage. Human Relations, 45(7), 659-686.

Bejger, S., & Elster, S. (2020). Artificial intelligence in economic decision making: How to assure a trust? Ekonomia I Prawo, 19(3), 411. https://doi.org/10.12775/eip.2020.028

Bokhari, S. A. A., & Myeong, S. (2023, March). Ai applications in smart city employing technology adoption model: Hofstede's cultural perspective. In 2023 2nd International Conference for Innovation in Technology (INOCON) (pp. 1-6). IEEE.

Bor, S., & Koech, N. C. (2023). Balancing Human Rights and the Use of Artificial Intelligence in Border Security in Africa. J. Intell. Prop. & Info. Tech. L., 3, 77.

Bozkurt, A.; Karadeniz, A.; Baneres, D.; Guerrero-Roldán, A.E.; Rodríguez, M.E. Artificial Intelligence and Reflections from Educational Landscape: A Review of AI Studies in Half a Century. Sustainability 2021, 13, 800. https://doi.org/10.3390/ su13020800

Chen, X., Wang, Y., & Zhang, Z. (2019). "An AI-Based Decision Support System for Urban Flood Control." IEEE Transactions on Intelligent Transportation Systems, 20(5), 1963-1976.

Chiu, T. K., Ahmad, Z., Ismailov, M., & Sanusi, I. T. (2024). What are artificial intelligence literacy and competency? A comprehensive framework to support them. Computers and Education Open, 6, 100171.

Choudhury, A., Saremi, M. L., & Urena, E. (2023). Perception, trust, and accountability affecting acceptance of artificial intelligence: from research to clinician viewpoint. In Diverse Perspectives and State-of-the-Art Approaches to the Utilization of Data-Driven Clinical Decision Support Systems (pp. 105-124). IGI Global.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly, 319-340.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. Journal of Management Information Systems, 19(4), 9-30.

El-Emary, I., Al Otaibi, S., & Al Amri, W. (2020). The effect of using artificial intelligence on the quality of decision-making in various organizations: A critical survey study. Bioscience Biotechnology Research Communications, 13(4), 2042-2049. https://doi.org/10.21786/bbrc/13.4/61

Forster, M. (2023). Refugee protection in the artificial intelligence era. A test case for rights'(Chatham House, September 2022) < https://www. chathamhouse. org/sites/default/files/2022-09/2022-09-07-refugee-protection-artificial-intelligence-era-forster. pdf> accessed, 15.

Franke, G., & Sarstedt, M. (2019). Heuristics versus statistics in discriminant validity testing: A comparison of four procedures. Internet Research, 29(3), 430-447. https://doi.org/10.1108/IntR-12-2018-0563

Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. Communications of the association for information systems, 4(1), 7.

Gökalp, Y., Dinçer, H., Eti, S., & Yüksel, S. (2024). Generating a novel artificial intelligence-based decision-making model for determining priority strategies for improving community health. Journal of Operations Intelligence, 2(1), 1-13.

Goli, M., Sahu, A. K., Bag, S., & Dhamija, P. (2023). Users' acceptance of artificial intelligence-based chatbots: an empirical study. International Journal of Technology and Human Interaction (IJTHI), 19(1), 1-18.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2020). Multivariate data analysis (8th ed.). Cengage Learning.

Ho, M. T., Nguyen, M. H., & Vuong, Q. H. (2022). Sociocultural factors influence young people's attitude towards the harvesting of non-conscious emotional data.

Hung, S. Y., & Wu, H. L. (2012). Factors influencing user acceptance of web-based decision support systems. Journal of Computer Information Systems, 52(4), 70-77.

Islam, M.R.; Ahmed, M.U.; Barua, S.; Begum, S. A Systematic Review of Explainable Artificial Intelligence in Terms of Different Application Domains and Tasks. Appl. Sci. 2022, 12, 1353. https://doi.org/ 10.3390/ app12031353

Kacprzyk, J. (2022, December). AI-enabled Decision Aid and Decision Support for Symbiotic Autonomous Systems. In 2022 IEEE 21st International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC) (pp. 4-5). IEEE.

Karen Neville, Sheila O'Riordan, Andrew Pope, Marion Rauner, Maria Rochford, Martina Madden, James Sweeney, Alexander Nussbaumer, Nora McCarthy & Cian O 'Brien (2016) Towards the development of a decision support system for multi-agency decision-making during cross-border emergencies, Journal of Decision Systems, 25:sup1, 381-396, DOI:

10.1080/12460125.2016.1187393

Karolina, La, Fors., Fran, Meissner. (2022). Contesting border artificial intelligence: Applying the guidance-ethics approach as a responsible design lens. Data & policy, 4 doi: 10.1017/dap.2022.28

Kerimovs, A. (2024). Artificial Intelligence (AI) Model Development Framework for the Protection of State Borders, with a Focus on Analyzing Behavioral Patterns.

Kolidakis, S., Botzoris, G., Profillidis, V., & Kokkalis, A. (2020). Real-time intraday traffic volume forecasting–a hybrid application using singular spectrum analysis and artificial neural networks. Periodica Polytechnica Transportation Engineering, 48(3), 226-235.

Lederer, A. L., Maupin, D.J., Sena, M.P., & Zhuang, Y. (2000). The technology acceptance model and the world wild web. Decision Support Systems, 29 (3), 269-282.

Li, M., Liu, W., & Wang, H. (2018). "Integration of Weather Forecasting and Hydrological Modeling for Flood Prediction: A Case Study in a Mountainous Watershed." Water Resources Research, 54(9), 6321-6337.

Liehner, G. L., Biermann, H., Hick, A., Brauner, P., & Ziefle, M. (2023). Perceptions, attitudes and trust towards artificial intelligence—an assessment of the public opinion. Artificial Intelligence and Social Computing, 72(72).

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. Information systems research, 2(3), 173-191.

Panicker, R. O., & George, A. E. (2023). Adoption of Automated Clinical Decision Support System: A Recent Literature Review and a Case Study. Archives of Medicine and Health Sciences, 11(1), 86-95.

Pelau, C., Dabija, D. C., & Ene, I. (2021). What makes an AI device human-like? The role of interaction quality, empathy and perceived psychological anthropomorphic characteristics in the acceptance of artificial intelligence in the service industry. Computers in Human Behavior, 122, 106855. https://doi.org/10.1016/j.chb.2021.10685

Ramayah, T., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2018). Partial least squares structural equation modeling (PLS-SEM) using SmartPLS 3.0: An updated guide and practical guide to statistical analysis (2nd ed.). Pearson Education Limited.

Salim, S. (2024, April 26). Heaviest rain in UAE "most disruptive weather event" in 63-year history of Dubai airport - News | Khaleej Times. Khaleej Times. https://www.khaleejtimes.com/uae/weather/heaviest-rain-in-uae-most-disruptive-weather-event-in-63-year-history-of-dubai-airport?_refresh=true

Sanja, Milivojevic. (2022). Artificial intelligence, illegalised mobility and lucrative alchemy of border utopia. Criminology & Criminal Justice, 174889582211238-174889582211238.doi:10.1177/17488958221123855

Smith, A., Jones, B., & Johnson, C. (2020). "Application of Machine Learning Techniques in Flood Risk Management: A Review." Journal of Hydroinformatics, 22(3), 548-565.

Stone, M., Aravopoulou, E., Ekinci, Y., Evans, G., Hobbs, M., Labib, A., ... Machtynger, L. (2020). Artificial intelligence (AI) in strategic marketing decision-making: a research agenda. The Bottom Line, 33(2), 183-200. https://doi.org/10.1108/BL-03-2020-0022

Taylor, S., & Todd, P. (1995). Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions. International journal of research in marketing, 12(2), 137-155.

Tosin, Ige., Abosede, Kolade., Olukunle, Kolade. (2023). Enhancing Border Se-

curity and Countering Terrorism Through Computer Vision: a Field of Artificial Intelligence. arXiv.org, abs/2303.02869:656-666. doi: 10.1007/978-3-031-21438-7_54

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management science, 46(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. Journal of the Association for Information Systems, 17(5), 328-376.

Yi, M., & Choi, H. (2023). What drives the acceptance of AI technology?: the role of expectations and experiences. arXiv preprint arXiv:2306.13670.

Appendix A: Operationalization

Table 1. Operationalization of the constructs

Construct	Code	Statement in Arabic	Statement in English
System Design	SD1	واجهة النظام سهلة الاستخدام	The system interface is easy to use.
System Design	SD2	ميزات النظام متكاملة بشكل جيد	The system features are well integrated.
System Design	SD3	النظام موثوق ونادراً ما يتعطل	The system is reliable and rarely crashes.
System Design	SD4	النظام قابل للتخصيص لتلبية احتياجاتي	The system is customizable to meet my needs.
System Design	SD5	النظام يتكامل جيدًا مع الأنظمة الأخرى التي أستخدمها	The system integrates well with other systems I use.
Perceived Ease of Use	PEU1	تعلم تشغيل النظام سهل بالنسبة لي	I have no trouble learning how to use the system.
Perceived Ease of Use	PEU2	النظام سهل الاستخدام	Using the system is simple.
Perceived Ease of Use	PEU3	من السهل أن أصبح ماهراً في استخدام النظام	Gaining proficiency with the system is simple.
Perceived Ease of Use	PEU4	التفاعل مع النظام لا يتطلب الكثير من الجهد العقلي	It takes little brain effort to interact with the system.
Perceived Ease of Use	PEU5	النظام يقدم معلومات واضحة ومفهومة	The system provides clear and understandable information.
Behavioral Intention to Use	BIU1	أنوي استخدام النظام بانتظام في المستقبل	In the future, I plan to make frequent use of the system. mation.
Behavioral Intention to Use	BIU2	سأوصي الآخرين باستخدام النظام	I would recommend others to use the system.
Behavioral Intention to Use	BIU3	أخطط لزيادة استخدامي للنظام	I plan to increase my use of the system.
Behavioral Intention to Use	BIU4	سأستمر في استخدام النظام في عملي	I›ll keep using the system for my job.

Organizational Support	BIU1	توفر مؤسستي الموارد الكافية لاستخدام النظام المدفوع بالذكاء الاصطناعي	My organization provides sufficient resources for using the AI-driven system.
Organizational Support	BIU1	هناك فريق دعم متخصص لمساعدة في القضايا المتعلقة بالنظام المدفوع بالذكاء الاصطناعي	There is a specialized support team to assist with AI system issues.
Organizational Support	BIU1	مؤسستي تشجع على استخدام النظام المدفوع بالذكاء الاصطناعي	The AI-driven system is encouraged to be used by my organization.
Organizational Support	BIU1	تتوفر برامج تدريبية لمساعدة الموظفين على تعلم استخدام نظام المدفوع بالذكاء الاصطناعي بفعالية	To help staff members become proficient with the AI-driven system, training courses are offered.

Note. * 1= Strongly Disagree; 2= Disagree; 3= Neutral; 4= Agree; 5= Strongly Agree

Appendix B: HTMT

Table 2. HTMT

	1	2	3	4
1. AI Adoption (AI)	-			
2. Organizational Support (OS)	.78	-		
3. Perceived Ease of Use (PEU)	.849	.64	-	
4. System Design (SD)	.849	.784	.836	-

Appendix C: Hypothesis Testing

Table 3. Hypothesis Testing

Hypothesisport	Path Description	Std. Beta	Std. Error	t-value	p-value	Q^2predict	RMSE	Decision
H1	System Design (SD) -> Perceived Ease of Use (PEU)	.73	.07	9.98	.00	.59	.59	Supported
H2	Organizational Support (OS) -> Perceived Ease of Use (PEU)	.12	.08	1.38	.165	N/A	N/A	Not Supported

Note. N/A Not Applic

References:

1. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.

- This foundational paper introduces the original TAM and provides scales for perceived usefulness and perceived ease of use.

2. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. Management Science, 46(2), 186-204.

- This paper extends the TAM model and includes refined scales for measuring perceived usefulness, perceived ease of use, and behavioral intention to use.

3. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.

- This paper introduces the Unified Theory of Acceptance and Use of Technology (UTAUT) and provides validated scales for measuring constructs similar to those in TAM.

4. Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. Management Science, 35(8), 982-1003.

- This study compares TAM with other models and provides additional insights into measuring perceived usefulness and perceived ease of use.

5. Chin, W. W., & Gopal, A. (1995). Adoption intention in GSS: Relative importance of beliefs. Data Base for Advances in Information Systems, 26(2-3), 42-64.

- This paper provides scales and insights for measuring behavioral intention to use technology.

6. Agarwal, R., & Prasad, J. (1999). Are individual differences germane to the acceptance of new information technologies? Decision Sciences, 30(2), 361-391.

- This study examines individual differences and their impact on technology acceptance, providing useful scales and constructs.

7. Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. Information Systems Research, 2(3), 192-222.This paper develops an instrument for measuring perceptions of IT adoption, which can be useful for creating items related to system design and perceived usefulness.
8. Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157-178.This extension of UTAUT includes new constructs and scales that can be relevant for studying AI-driven decision support systems.
9. Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. MIS Quarterly, 19(2), 189-211.
10. Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a research agenda on interventions. Decision Sciences, 39(2), 273-315.
11. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.
12. Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. MIS Quarterly, 15(1), 125-143.
13. Igbaria, M., & Iivari, J. (1995). The effects of self-efficacy on computer usage. Omega, 23(6), 587-605.
14. Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a research agenda on interventions. Decision Sciences, 39(2), 273-315.

Appendix D: Questionnaire (Translated).

استبانة حول استخدام نظم دعم القرار المدفوعة بالذكاء الاصطناعي مستقبلًا (DSS) من قبل الهيئة الاتحادية للهوية والجنسية والجمارك وامن المنافذ

تم تصميم هذه الاستبانة للتعرف على استخدام نظم دعم القرار المدفوعة بالذكاء الاصطناعي مستقبلا من الهيئة وذلك بهدف تعزيز الاستفادة من تطبيقات الذكاء الاصطناعي في التقليل من اثار الازمات والكوارث المحيطة بالمنافذ البرية والبحرية والجوية لدولة الامارات العربية المتحدة

يرجى الإجابة على كافة العبارات الواردة بوضع علامة بجانب الاختيار المناسب، ونحيطكم علماً بأن جميع المعلومات سيتم استخدامها للأغراض الاكاديمية وللبحث والتطوير، وستعامل بسرية تامة.

ونشكر لكم تعاونكم.

1. المعلومات الديموغرافية

1. النوع الاجتماعي؟

- ☐ ذكر
- ☐ أنثى

2. الخبرة العملية؟

- ☐ أقل من 5 سنوات
- ☐ سنوات10 - 5
- ☐ من 10 سنوات فأكثر

3. مجال الوظيفة؟

- ☐ ضابط (تفتيش، تحليل، استهداف، تقييم)
- ☐ قيادي (مدير/نائب مدير/مدير مكتب/مدير قسم أو فرع/مسؤول)
- ☐ موظف دعم (تقني/الفني/اداري)

4. مقر العمل؟

- ☐ المنافذ الجوية
- ☐ المنافذ البحرية
- ☐ المنافذ البرية
- ☐ تابع للمقر الرئيسي للهيئة

2. تصميم النظام

1. واجهة النظام سهلة الاستخدام

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

2. ميزات النظام متكاملة بشكل جيد.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

3. النظام موثوق ونادراً ما يتعطل.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

4. النظام قابل للتخصيص لتلبية احتياجاتي.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

5. النظام يتكامل جيدًا مع الأنظمة الأخرى التي أستخدمها.

- ☐ أوافق بشدة
- ☐ أوافق

- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

3. سهولة الاستخدام المتصورة للنظام

1. تعلم تشغيل النظام سهل بالنسبة لي.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

2. النظام سهل الاستخدام.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

3. من السهل أن أصبح ماهراً في استخدام النظام.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

4. التفاعل مع النظام لا يتطلب الكثير من الجهد العقلي.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

5. النظام يقدم معلومات واضحة ومفهومة.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

4. النية السلوكية للاستخدام النظام

1. أنوي استخدام النظام بانتظام في المستقبل.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

2. سأوصي الآخرين باستخدام النظام.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

3. أخطط لزيادة استخدامي للنظام.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

4. سأستمر في استخدام النظام في عملي.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد

- ☐ لا أوافق
- ☐ لا أوافق بشدة

5. الدعم التنظيمي

1. توفر مؤسستي الموارد الكافية لاستخدام نظام DSS المدفوع بالذكاء الاصطناعي.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

2. هناك فريق دعم متخصص لمساعدة في القضايا المتعلقة بنظام DSS المدفوع بالذكاء الاصطناعي.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

3. مؤسستي تشجع استخدام نظام DSS المدفوع بالذكاء الاصطناعي.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

4. تتوفر برامج تدريبية لمساعدة الموظفين على تعلم استخدام نظام DSS المدفوع بالذكاء الاصطناعي بفعالية.

- ☐ أوافق بشدة
- ☐ أوافق
- ☐ محايد
- ☐ لا أوافق
- ☐ لا أوافق بشدة

بحث بعنوان :

التفريد القضائي وأثره في تحقيق مقصد الشارع من العقاب.

د. محمد إسحاق الخاجه
باحث أكاديمي
الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ

الملخص

تهدف هذا الدراسة إلى التعرف على أثر التفريد القضائي في تحقيق مقصد الشارع من العقاب وفق ما نص عليه مرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب في دولة الإمارات العربية المتحدة، ولتحقيق الدراسة أهدافها اعتمدت على المنهج التأصيلي من خلال استقراء الموضوعات الجزئية المتعلقة بموضوع الدراسة من كتاب الله -سبحانه وتعالى- والسنة النبوية، وكتب التفسير والفقه والسير، والكتب والأبحاث المحكمة والمقالات المختصة ذات الصلة بموضوع الدراسة، والمراجع العلمية سواء أكانت فقهية أو قانونية، والمنهج التحليلي وذلك من خلال تطبيق القواعد والمبادئ العامة التي تحكم التفريد القضائي للعقوبة والمرتبطة بسياسة المشرع العقابية في المرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب.

توصلت الدراسة إلى مجموعة من النتائج لعل أهمها أن الفقه الجنائي الإسلامي عرف مضامين التفريد القضائي منذ قرون عديدة، والتي كان لها أثر في تحقيق مقصد الشارع من العقاب، أمّا التوصية فتتمثل في مقترح للمشرع الاتحادي في دولة الإمارات العربية المتحدة إلى تعديل نص المادة (32) من المرسوم بقانون رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب، بحيث يسمح للقاضي الجنائي بممارسة سلطته التقديرية في التفريد القضائي.

الكلمات المفتاحية: التفريد القضائي، العقوبة، سلطة القاضي الجنائي.

Abstract

This study aims to examine the impact of judicial individualization on achieving the purpose of punishment as intended by the Emirate legislator, according to the provisions of Federal Decree-Law No. (29) of 2021 concerning the entry and residence of foreigners in the United Arab Emirates. To achieve its objectives, the study adopts a foundational methodology by exploring specific topics related to the study from the Holy Qur'an, the Sunnah of the Prophet (peace be upon him), and from books of interpretation, jurisprudence, biographies, as well as peer-reviewed research, specialized articles, and scientific references, whether legal or jurisprudential. The analytical method was also employed by applying the general principles and rules governing judicial individualization of

punishment, directly related to the theory of punishment as stated in Federal Decree-Law No. 29 of 2021 regarding the entry and residence of foreigners. The study concluded with several findings, the most notable of which is that Islamic criminal jurisprudence has recognized the concept of judicial individualization for centuries, which has significantly contributed to achieving the purpose of punishment as intended by the legislator. The key recommendation is for the federal legislator in the UAE to repeal Article (32) of Federal Decree-Law No. (29) of 2021 concerning the entry and residence of foreigners.

Keywords: Judicial Individualization, Punishment, authority of the criminal judge.

المقدمة

يشكل مبدأ التفريد القضائي للعقوبة أحد أهم المبادئ الرئيسية في القانون الجنائي المرتبطة بصورة مباشرة بنظرية العقاب، حيث يهدف هذا المبدأ إلى تحقيق العدالة الجنائية من خلال معاقبة كل جانٍ بالعقوبة المستحقة

والحديث عن التفريد القضائي يستلزم البحث في معادلة معقدة تتكون من ثلاث متغيرات غير ثابتة في علم الإجرام والعقاب، وهي: الجريمة، والمجرم، والعقوبة، ولعلها – العقوبة - هي المجهول الأصعب بسبب تضارب النظريات المتعددة والمتناقضة في تفسير الفلسفة الكامنة وراء تشريع العقاب

كانت المدرسة التقليدية القديمة هي السائدة في تحديد الفلسفة العقابية، والمتمثلة في ضرورة تطبيق العقوبة على مرتكب الجريمة، لأن ذلك يستوجب العدل، ويفرض ضرورة التأكيد على رفض المجتمع للتصرف الإجرامي، حيث كانت العقوبة هي الرد الحتمي للجريمة، وكانت سلطة القضاء مطلقة، فاتسمت العقوبة بطابع القصاص والانتقام، وازدادت أهمية عقوبة الإعدام والعقوبات السالبة للحرية طويلة الأمد أو المؤبدة، حيث تؤدي في النهاية إلى إبعاد المحكوم عليه عن المجتمع، لذلك كانت الدراسات العقابية في هذه المرحلة تُسمى «علم السجون "Science Penitentiaire»، ومن هنا كان من غير الممكن ظهور مصطلح التفريد القضائي في ذلك المجتمع آنذاك (حسني (1972)، ص 91)

إلا أن ظهور المدارس الحديثة وتطور العلوم الجنائية انعكس على تطور في تحديد الفلسفة الكامنة وراء العقاب، بالإضافة إلى الأصوات المطالبة باحترام حقوق الإنسان والنظر إلى المجرم باعتباره مريضًا يجب معالجته، هذا إلى جانب فشل السياسات العقابية القديمة في تحقيق الأهداف المرجوة من العقاب، مثل منع الجريمة أو التقليل منها، كل ذلك مهد الطريق لظهور نظريات جديدة تركز على المجرم لا على الجريمة (التميمي (2016)، ص 122)

يقول بنتام «إن العقاب وإن كان واحدًا في الاسم، يختلف في الحقيقة باختلاف النوع والسن والمنزلة والثروة، وغير ذلك من الأحوال، مثال ذلك لو عوقب على الضرب بالغرامة، لكانت العقوبة بالنسبة للغني عبثًا، وبالنسبة للفقير ظلمًا، وكذلك العقاب إن كان مخلاً بالكرامة بطبيعته، يكون قاسيًا بالنسبة لذي المكانة، ولا يصيب الطبقة التي تكون من دون ذلك بشيء، والحبس خراب لذي متجر، وإعدام لشيخ هرم، وعار أبدي للنساء، ولا يكون فيه شيء من ذلك لقوم آخرين» (بنتام، 1999، ص: 233)

وهكذا بدأت الأبحاث والدراسات النظرية تتوالى في هذا الجانب بحثًا عن أنجح الوسائل لإصلاح الجاني، باعتباره أهم أهداف العقاب، وظل هذا التطور الكبير في الدراسات الجنائية والعقابية سعيًا لجعل العقوبة ملائمة لشخصية المجرم والدوافع الكامنة وراء ارتكاب الجريمة، كل ذلك مهد لظهور مصطلح التفريد القضائي (سلامة، 1975، ص 6).

1.1 تساؤلات موضوع الدراسة:

ستُجَّيب هذه الدراسة على التساؤل الرئيسي الآتي:

ما أثر التفريد القضائي في تحقيق مقصد المشرع الإماراتي من العقاب وفق ما نص عليه مرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بدولة الإمارات العربية المتحدة؟

ومن ثم سنتفرع للأسئلة الفرعية الآتية:

(1) ما المقصود من مصطلح (التفريد القضائي)؟

(2) ما التأصيل الشرعي لمصطلح التفريد القضائي؟

(3) ما نطاق هذا المصطلح في الفقه الجنائي الإسلامي؟

(4) وما أثر العمل بالتفريد القضائي في تحقيق مقصد المشرع من العقاب؟

1.2 أهمية موضوع الدراسة:

(1) الأولى من نوعها على مستوى دولة الإمارات العربية المتحدة والتي تناولت مبدأ التفريد القضائي في مرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب.

(2) الإجابة عن الأسئلة التي طرحتها مشكلة الدراسة.

(3) بيان ثراء الشريعة الإسلامية وتفوقها على كافة القواعد والمبادئ والنظريات الكبرى التي ينهض عليها الفقه الجنائي الحديث.

(4) ترفد المكتبة القانونية بالهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ بمساهمة جديدة يحتاجها المهتمون بموضوع الدراسة، من خلال طرح موضوع الدراسة من الجانب الشرعي وعدم الاقتصار على عرض الموضوع من جوانبه القانونية والوضعية.

1.3 أهداف موضوع الدراسة:

(1) التعرف على أثر التفريد القضائي في تحقيق مقصد الشارع الإماراتي من العقاب وفق ما نص عليه مرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول

وإقامة الأجانب في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ في دولة الإمارات العربية المتحدة.

(2) التعرف على المقصود من مصطلح التفريد القضائي.

(3) دراسة وتحليل وتأسيس الموضوعات الجزئية المتعلقة بالتفريد القضائي وردّها إلى القاعدة العامة التي تحكمها.

(4) التعرف على حدود تطبيق التفريد القضائي في الفقه الجنائي الإسلامي.

(5) قياس أثر التفريد القضائي في تحقيق مقصد المشرع من العقاب.

1.4 حدود الدراسة:

تمثلت حدود الدراسة فيما يلي:

(1) الحدود المكانية: اقتصرت هذه الدراسة على مرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب.

(2) الحدود الزمنية: اقتصرت هذه الدراسة خلال العام 2024-1445هـ.

1.5 مراجعة الأدبيات والدراسات السابقة:

الدراسة الأولى: بحث منشور في مجلة الدراسات القضائية التابعة لوزارة العدل في دولة الإمارات العربية المتحدة، العدد الخامس والعشرون السنة الرابعة عشر، جمادى الأولى 1445هـ – ديسمبر 2023م، وعنوان البحث: **التفريد القضائي للعقوبة في التشريع الإماراتي،** سعود عبد القادر الشاعر.

وقد عمل الباحث على إبراز السلطة التقديرية للقاضي في إيقاع العقوبة على المتهم في قانون دولة الإمارات العربية المتحدة، ومدى تعارض هذه السلطة التقديرية مع مبدأ الشرعية.

ورغم أهمية البحث وإسهامه في تسليط الضوء على مصطلح التفريد القضائي في دولة الإمارات العربية المتحدة إلا أنه لا يغني عن بحثي هذا لما تضمنه هذا البحث من إضافات هامة تتعلق بالفلسفة التي قام عليها النظام العقابي في الشريعة الإسلامية، والمرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب في دولة الإمارات العربية المتحدة.

الدراسة الثانية: بحث منشور في المجلة الأردنية للدراسات الإسلامية، المجلد (12)، العدد 2، 1437هـ/2016م وعنوان البحث: **التفريد الجزائي: مفهومه وتأصيله على ضوء مقاصد الشارع من العقاب،** عماد محمد رضا على التميمي.

وقد عمل الباحث على إبراز الفلسفة التي قام عليها النظام العقابي في الفقه الإسلامي، مبيناً مفهوم مصطلح التفريد الجزائي، والتأصيل الشرعي لهذا المصطلح القانوني، والحكم

عليه من خلال عرضه على تلك الفلسفة العقابية والنظر في المآلات التي ينتهي إليها.
ورغم أهمية البحث وإسهامه في تسليط الضوء على مصطلح التفريد الجزائي إلا أنه لا يغني عن بحثي هذا لما تضمنه هذا البحث من إضافات هامة تتعلق بالفلسفة التي قام عليها النظام العقابي في مرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب في دولة الإمارات العربية المتحدة

الدراسة الثالثة: بحث منشور في المجلة الأردنية للدراسات الإسلامية، المجلد الخامس، العدد 1، 1430هـ/2009م وعنوان البحث: فردية العقاب بين نظرية الدفاع الاجتماعي والفقه الإسلامي، محمد نوح معابدة

وقد عمل الباحث على إبراز جوانب نظرية الدفاع الاجتماعي السائدة في عالم الجريمة والعقاب في الفقه الجنائي الوضعي وربط تلك الجوانب بما هو مقرر في الفقه الجنائي الإسلامي، وأثبت الباحث في نهاية بحثه مقارنة بين ما هو مقرر في الشريعة الإسلامية منذ قرون – في هذا الجانب- وبين ما دعت إليه النظرية في العصر الحديث.

الدراسة الرابعة: رسالة دكتوراه في السياسة الجنائية صادرة عن وزارة التعليم العالي في الجمهورية الجزائرية، مدرسة الدكتوراه للعلوم القانونية والإدارية، 2009/2008م، وعنوان البحث: **تفريد الجزاء الجنائي، للباحث بديار ماهر**

وقد أسهب الباحث في الحديث عن المصطلح من جوانبه القانونية الوضعية، إلا أن البحث يفتقر إلى التأصيل الشرعي للمصطلح وتسليط الضوء عليه من خلال ما هو مقرر من القواعد العامة في الفقه الجنائي الإسلامي، وما قام عليها النظام العقابي في المرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب في دولة الإمارات العربية المتحدة.

الدراسة الخامسة: رسالة ماجستير صادرة عن المركز العربي للدراسات الأمنية والتدريب، الرياض، 1414-1415هـ، وعنوان الرسالة: **السلطة التقديرية للقاضي في تفريد العقوبة في مجال التعزير،** للباحث: حامد حسن متروك الجهني

وقد تناول الباحث في دراسته أشكال التفريد بصفة عامة ثم حصر دراسته في التفريد القضائي، ورغم أهمية الدراسة في هذا الجانب إلا أنها لا تغني عن دراستي، إذ دراستي تتناول تأصيل المصطلح وتكييفه الفقهي وفق الفلسفة التي قام عليها النظام العقابي في الإسلام والمرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب في دولة الإمارات العربية المتحدة.

1.6 منهجية البحث وأدواته:

تعتمد هذه الدراسة على المناهج الآتية:

أولاً: المنهج التأصيلي، وذلك من خلال استقراء الموضوعات الجزئية المتعلقة بموضوع الدراسة من كتاب الله -سبحانه وتعالى- والسنة النبوية، وكتب التفسير والفقه والسير، والكتب والأبحاث المحكمة والمقالات المختصة ذات الصلة بموضوع الدراسة، والمراجع العلمية سواء أكانت فقهية أو قانونية

ثانياً: المنهج التحليلي، وذلك من خلال تطبيق القواعد والمبادئ العامة التي تحكم التفريد القضائي للعقوبة والمرتبطة بصورة مباشرة بنظرية العقوبة في المرسوم بقانون اتحادي رقم 29 لسنة 2021 في شأن دخول وإقامة الأجانب، وبعض الأحكام القضائية في هذا الصدد

1.7 هيكلة الدراسة وتقسيماتها:

سيتناول الباحث موضوع الدراسة من خلال مطلب تمهيدي، ومبحثين على النحو الآتي:

(1) **المقدمة:** وتشمل مشكلة الدراسة وتساؤُلاتها، وأهداف الدراسة وأهميتها، ومصطلحات الدراسة وحدودها، ومنهجية الدراسة وأدواتها، وهيكلة الدراسة وتقسيماتها.

(2) **المبحث الأول:** ماهية التفريد القضائي لدى الفقه الإسلامي وفي القانون الوضعي.

(3) **المبحث الثاني:** التفريد التشريعي وفقاً لما نص عليه المرسوم، وعلى ضوء سلطة القاضي الجنائي التقديرية في تطبيقه.

(4) **الخاتمة:** وتتضمن نتائج الدراسة وتوصياتها.

المطلب التمهيدي

- **تطور مفهوم وفلسفة التفريد القضائي في الفكر العقابي**

التفريد العقابي يكون بإخضاع كل مجرم بحسب ظروفه الشخصية أو خطورته الإجرامية لما يلائمه من تدابير وقائية وعلاجية وتربوية تضمن إعادة إصلاحه ودمجه في المجتمع (علي، راشد، 1964، ص 215)، وهو يُقسم إلى تفريد تشريعي، وتفريد قضائي، وتفريد تنفيذي، وباستقراء نظريات علم الإجرام والعقاب وعلاقتها بالفكر العقابي نجد بأن سياسة العقاب تأثرت بالأفكار الفلسفية والقيم السائدة في تلك العصور، وهذا انعكس أثره على التفريد القضائي في هذه المجتمعات الغربية، حيث كانت سلطة القضاء مطلقة في تقدير العقوبة في العصور القديمة، ومن ثم تقيدت هذه السلطة في عهد المدرسة التقليدية، وصولاً إلى السلطة النسبية

وعليه تأتي أهمية هذه الدراسة في إلقاء الضوء على تطور هذه الفلسفة العقابية وأثرها في نشوء مصطلح التفريد القضائي من خلال تناول هذا التطور الفقهي والقانوني لهذه النظم المتتابعة، على النحو التالي

الفرع الأول

- **السلطة المطلقة للتفريد القضائي**

بدأت في العصور القديمة، قبل الثورة الفرنسية التي كانت في القرن الثامن وكانت السياسة العقابية تتجه نحو الشدة والعنف، وكانت السلطة القضائية تمارس من قبل شخص واحد مثل رب الأسرة أو رئيس القبيلة، وفي الحضارات القديمة كانت السلطة القضائية تمارس من قبل الحاكم أو القاضي - الملوك أو أعوانهم من الطبقة الأرستقراطية - أو الكهنة، وكان لهم السلطة المطلقة في الفصل في المنازعات المدنية أو الجنائية، دون مراعاة لأي قواعد قانونية (السعيد (1962)، الأحكام العامة في قانون العقوبات، ص: 94- 100).

وغلب على قوانين هذا العصر الطابع الديني وتقيُد السلطة القضائية بالشرائع الدينية والأعراف، وكان الغرض من العقوبة التكفير عن عصيان المجرم، وتُطبق بشكل إلزامي لكسب رضا الإله والردع العام، وعلى الرغم من ذلك كانت السلطة القضائية تفسر هذه الشرائع والأعراف عند تطبيقها تفسير يوافق رغباتهم حينئذ، وكان يُنظر إليهم على أنهم ممثلو للعدالة الإلهية أو سيادة الدولة

وفي القرن السادس عشر ظهرت العقوبات التحكمية في فرنسا كمظهر من السلطة

المطلقة للتفريد القضائي، وهي جرائم وعقوبات منصوص عليها في أمر ملكي مع منح القاضي سلطة مطلقة لتوقيع أي عقوبة أخرى أشد، على أن تكون من ضمن العقوبات المقررة بموجب الأوامر الملكية أو بمقتضى السوابق القضائية، وعقوبات يوقعها أعضاء السلطة القضائية على مرتكبي الأفعال التي يرون تجريمها، دون أن يسبق تجريم تلك الأفعال بمقتضى الأوامر الملكية أو السوابق القضائية للمحكمة العليا، بشرط أن تكون هذه العقوبات من ضمن العقوبات المقررة في المملكة.

وسادت هذه العقوبات التحكمية على العقوبات الثابتة المنصوص عليها في الأوامر الملكية، والتي أهمل القضاء تطبيقها تدريجيا، وأصبح التفريد العقابي متروكاً للسلطة القضائية بصورة مطلقة، وعليه لم يكن هناك قانون عقوبات فعلي في فرنسا خلال تلك الحُقبة، ولم تكن الجرائم والعقوبات محددة في القانون نفسه تحديدا حاسماً (jousse, 11. P 599) ، وكذلك الحال في ألمانيا حتى سادت حكم القضاة دون حدود (Franz, 1908, p: 404)

من سلبيات السلطة المطلقة للتفريد القضائي الاستبداد القضائي وتعسف السلطة القضائية وعدم اتباع معيار محدد لقياس التناسب بين الجسامة المادية للجريمة والجسامة المادية للعقوبة، ودون الالتفات إلى تكوين المجرم وحالته وظروفه، وبواعثه، والانحياز الشخصي للأحكام القضائية المتأثرة بمُحَابَاة الحاكم، وغياب الشفافية لعدم وجود قنوات لاستئناف الأحكام القضائية مما يجعلها نهائية لا يمكن الطعن عليها، والتفاوت في تطبيق القانون بسبب الاجتهادات القضائية (Kcal Garraud, 1906, p 41)، نتج عن ذلك الظلم والتطرف وعدم المساواة أمام القانون، وقسوة العقوبات و وحشيتها وزيادة عقوبة الإعدام، كل ذلك دعى المختصون في ذلك العصر للتحرك ضد هذا النظام القانوني المعيب، والظهور بنظام قانوني جديد لتفادي القصور الذي عانته المدرسة التقليدية وتفادي قصور السلطة المطلقة للتفريد القضائي والبدء بالعمل بنظام السلطة المقيدة للتفريد القضائي

الفرع الثاني

- **السلطة المقيدة للتفريد القضائي**

وعلى أثرها تجرد السلطة القضائية من كل سلطة تقديرية في التجريم والعقاب، ويقتصر دورها على النطق بنوع ومقدار العقوبة المحددة من قبل المشرع للجريمة المحددة في القانون.

هذا التحول نتج من أحد الأقطاب الفكرية الجنائية في المدرسة التقليدية التي

تأسست بعد قيام الثورة الفرنسية وظهور إعلان حقوق الإنسان في عام 1789م على يد مؤسسها بيكاريا، والذي طالب بتقنين النصوص العقابية، وأن يكون غرضها تحقيق الردع العام والردع الخاص، لا أن يكون التعذيب والتخويف كعقوبة بتر الأعضاء والحرق، بالإضافة إلى التناسب بين الجريمة والعقوبة، فكان اهتمامه متعلقاً بوسائل العقوبة دون الاهتمام بغاياتها، وأكد وجوب إقرار قاعدة قانونية الجرائم والعقوبات، ونص المُشرع على نوع ومقدار العقوبة المقررة تبعا لشدة وضرر الفعل الإجرامي؛ لتأمين المساواة بين المجرمين، بالإضافة إلى إقرار قاعدة الأصل في المتهم البراءة؛ والتي تعتبر من أهم النتائج غير المباشرة إلى تكريس السلطة التقديرية للقاضي الجزائي، وخاصة عند عدم كفاية الأدلة أو ضعفها، وإعمال قاعدة الشك يفسر لمصلحة المتهم وغيرها من القواعد الإجرائية (يحياوي، 2016، ص: 96)، وبالتالي تجريد القاضي من كل سلطة تقديرية في هذا المجال، وقد حلت أفكار بيكاريا في قانون عقوبات الثورة الفرنسية تلبية لنداءات الجماهير المطالبة برعاية حقوق الإنسان وضمان المساواة أمام القانون ضد تعسف الحكام وتحكم القضاة، وبذلك أصبحت سلطة التفريد القضائي مقيدة بعد أن كانت مطلقة(بيكاريا، 1764، ص: 123-124)

يُعاب على هذه السلطة المقيدة للتفريد القضائي أنها حجمت من دور السلطة القضائية واقتصرتها على تطبيق النصوص بصورة عامة وموحدة، دون دراسة الظروف الخاصة بالجريمة والمجرم، ودون أن يكون لها دور في تكييف العقوبة المناسبة على المجرم، لا شك أن ذلك يتنافى مع مبدأ العدالة المرجوة من القانون، لأن التطبيق الجامد للنصوص التجريمية يعني أن يبحث القاضي عن توافر أركان وشروط الجريمة فقط، دون النظر والبحث في الظروف الشخصية للمجرم، والبواعث على ارتكاب الجريمة، والملابسات المحيطة بكل مجرم وجريمة ودراستها بصورة مستقلة، ودون أن يكون له دور في تكييف العقوبة المناسبة على المجرم، فدوره مقتصر على تطبيق العقوبة المنصوص عليها في القانون حتى لو كانت متناقضة مع العدالة، مثال ذلك عقوبة السرقة فهي واحدة، وعليه فإن من سرق درهماً تكون عقوبته مثل عقوبة من يسرق ألف درهم

فبعد أن كان هدف هذا النظام المساواة بين المواطنين وتحقيق العدالة أمام القانون انحرف بعدالة العقاب نحو عدم المساواة بصورة بالغة؛ بسبب التقيد المطلق للتفريد القضائي وعدم دراسة الحالة الشخصية للمجرم، فالعقوبة قد تكون بسيطة لمجرم معتاد الإجرام، بينما تكون قاسية وشديدة على مجرم ارتكب الجريمة لأول مرة تحت أي ضغط أو ظروف مؤثر أرغمه على ارتكابها، كل ذلك استدعى لوجد تعاون بين السلطة التشريعية والسلطة القضائية، وعلى إثرها ظهر ما يعرف بالسلطة النسبية للتفريد القضائي.

الفرع الثالث

- **السلطة النسبية للتفريد القضائي**

في أواخر القرن التاسع عشر تمت دراسة الجريمة عن طريق المنهج العلمي التجريبي، وارتكزت الدراسة على شخصية المجرم كونه أساس الجريمة ومرتكبها، والظروف المساعدة للإجرام، وذلك كردة فعل بعد صدور القانون الفرنسي عام 1810م، والذي كان يتمحور حول تحقيق المصلحة الاجتماعية في تطبيق العقوبات، وعلى هذا الأساس اهتدى الفكر القانوني للمجتمعات إلى السلطة النسبية للتفريد القضائي (محده، 2004، ص35 -36)، وتغيرت النظرة من الجمود إلى المرونة، وبالتالي ظهر العديد من المفكرين الذين أسهموا في تطوير فكر المدرسة التقليدية وظهور المدرسة الوضعية التي نادت بالسلطة النسبية للتفريد القضائي في تقدير العقوبة على الجاني، ومن أشهر هؤلاء المفكرين « سيزار لومبروزو» و « أنريكو فيري»، وذلك نتيجة إخفاق المرحلتين السابقتين بين إفراط وتفريط، حيث أعطى هذا الفكر مرونة بين السلطة التشريعية والقضائية؛ فالمشرع مهما أوتي من علم ودراية وبعد نظر لن يكون بمقدوره أن يلم بكل سلوكيات الأفراد الضارة بمصالح المجتمع محل الحماية القانونية، ومن جهة أخرى فإن القاضي لا يستطيع الإلمام بجميع الملابسات والفرضيات الدالة على الخطورة الإجرامية الكامنة في شخص الجاني، وهذا الواقع هو الذي أدى إلى الاعتراف بالسلطة النسبية للتفريد القضائي (مباركي، دليلة، ص:88)

ويكون دور المشرع في تحديد أنواع العقوبات وفق السلطة النسبية عن طريق وضع الحد الأدنى والحد الأقصى للعقوبة أو عقوبات متعددة، ويأتي دور القاضي، لدراسة الظروف النفسية والشخصية للجاني والظروف المحيطة بالجريمة، ومن ثم تحديد العقوبة المناسبة للمجرم والقدر اللازم للعقوبة، وفق الإطار التشريعي المعمول به وغايات المشرع (المهرية (2022)، ص: 200)

من هنا اتجهت التشريعات الجنائية الحديثة إلى الأخذ بهذا الاتجاه، كون شخصية المجرم والظروف الاجتماعية وملابسات كل جريمة على حدة أصبحت محل نظر واعتبار، ويأتي بعده الدور الجوهري للقاضي بممارسة حريته في استنباط الحقيقة والبحث الواسع في الأدلة وتقديرها وقبولها، وتكوين قناعه حيادية ومنصفة للوصول إلى الحكم العادل الصحيح على أكبر قدر من الاجتهاد (قريمس، سارة، 2015، ص:18).

بناء على ما سلف، فإن مرحلة السلطة النسبية للتفريد القضائي هي من مظاهر انعكاس علم الإجرام والعقاب على قانون العقوبات وخاصة مبدأ إقرار السلطة التقديرية

للقاضي الجنائي في هذه المرحلة وشكل النصوص الجزائية التي جاءت متأثرة بنتائج علم الإجرام والعقاب في فهم أسباب الجريمة، وهذا يعين المشرع في وضع النصوص التي تكفل مكافحتها، والقاضي يستعين بدراسة أسباب الجريمة في فهمه للواقعة المعروضة فيساعده ذلك في التفريد بصورة تحقق الغرض من العقوبة.

المبحث الأول

- **التأصيل الشرعي لمصطلح «التفريد القضائي»**

سأتناول في هذا المبحث مفهوم التفريد القضائي للعقوبة (١) في الفقه الجنائي الإسلامي والفقه الوضعي، من حيث الفلسفة العقابية في الفقه الجنائي الإسلامي والجرائم الوضعية وأثرها في التفريد القضائي في مطلبين، الأول منهما سأتناول فيه مفهوم التفريد القضائي لدى الفقه الجنائي الإسلامي، وأخصص الثاني لمفهوم التفريد القضائي في الفقه الوضعي.

المطلب الأول

- **مفهوم التفريد القضائي لدى الفقه الجنائي الإسلامي**

لبيان مفهوم أي مصطلح يجب تناوله ابتداءً من حيث تقرير المعاني، وتقعيد القواعد، وكذلك تبنى المسائل الفقهية على أصولها العلمية، وعليه فإن التفريد في اللغة هو مصدر للفعل الثلاثي المزيد فيه بحرف واحد (فرّد) يفرّد تفريداً، فَرد (اسم) والجمع أَفْرَادٌ، وفُرَادَى، والفَرْدُ: واحد، وتر، متوحّد، وحيد، منفرد (ابن فارس (1979)، المجلد الرابع، ص: 500، والزبيدي (بدون تاريخ)، (المجلد الثامن، ص: 482).

قال الليث: الفرد ما كان وحده، يقال: فَرَدَ يَفرُدُ وأَفرَدتُه جعلته واحداً، ويقال: جاء القوم فراداً فرادى، أي واحداً واحداً، ويقال: فَرَدَ برأيه وأَفرَد وفَرَّد واتفرد بِمَعنَى انفرد به، ومنه: استَفردتُ الشيءَ، إذا أخذته فرداً لا ثاني له، ويقال فرد الدل تفريداً: إذا تفقه، واعتزل الناس، وخلا بمراعاة الأمر والنهي (الأزهري (2001)، مجلد 14/70) وابن منظور (بدون تاريخ)، (المجلد الثالث، ص: 332-333).

وعليه يتبين أن المعنى الذي يدور حول هذه المادة اللغوية (فرد) هو عندي انفراد والوحدة والتعيين والتحديد، وكلها تدل على تفريد الشخص وتخصيصه بشيء دون أن يكون لغيره مثله.

ومن خلال بحثي هذا لم أقف على تعريف مصطلح (التفريد) لدى فقهاء الشريعة الإسلامية القدامى، أما المحدثون فقد عرفه الدكتور وهبة الزحيلي بقوله : «مبدأ تفريد

العقاب القضائي في نطاق التعازير، أي: إصدار العقوبة الملائمة لكل فرد على حدة حسبما يلائمه ويزجره، فيحقق فكرة السلطة التقديرية للقاضي ويساير التطور» (الزحيلي (بدون تاريخ)، ص5343/7)، ويلاحظ على هذا التعريف أنه خاص بالتفريد القضائي، والذي يعتبر نوعاً من أنواع تفريد العقوبة، وقد أورد الدكتور هذا التعريف في سياق الحديث عن جرائم التعزير، والتي تتفق مع التفريد في أن كليهما يحدد عقوبة تتناسب مع شخصيته المجرم وجسامة وظروف الجريمة.

من أجل تلك الغاية قسمت الشريعة الإسلامية الجرائم إلى نوعين، جرائم حدود وجرائم التعازير، وعليه سأتناول فلسفة العقاب في الجرائم الحدية، وأثرها في التفريد القضائي في الفرع الأول، وفلسفة العقاب في جرائم التعزيز، وأثرها في التفريد القضائي على النحو الآتي:

الفرع الأول

فلسفة العقاب في الجرائم الحدية، وأثر ذلك في التفريد القضائي [2]

لقد قامت فلسفة العقاب في هذه الجرائم على الأسس الآتية:

أولاً: العقوبة هي الجزاء المقابل للجريمة:

وأساس هذه الفلسفة قائم على أن العقوبة هي الجزاء العادل للجريمة، وعليه فلا بد من توقيع العقوبة كلّما ثبت ارتكاب الجريمة، وقد ساق الفقهاء بعضاً من الأدلة الدالة على ما ذكرنا ومن ذلك:

1. قوله تعالى: «إِنَّمَا جَزَاء الَّذِينَ يُحَارِبُونَ اللَّهَ وَرَسُولَهُ وَيَسْعَوْنَ فِي الأَرْضِ فَسَادًا أَن يُقَتَّلُواْ أَوْ يُصَلَّبُواْ أَوْ تُقَطَّعَ أَيْدِيهِمْ وَأَرْجُلُهُم مِّنْ خِلافٍ أَوْ يُنفَوْا مِنَ الأَرْضِ ذَلِكَ لَهُمْ خِزْيٌ فِي الدُّنْيَا وَلَهُمْ فِي الآخِرَةِ عَذَابٌ عَظِيمٌ﴾[المائدة: 33].
2. قوله تعالى: ﴿وَالسَّارِقُ وَالسَّارِقَةُ فَاقْطَعُواْ أَيْدِيَهُمَا جَزَاء بِمَا كَسَبَا نَكَالاً مِّنَ اللَّهِ وَاللَّهُ عَزِيزٌ حَكِيمٌ﴾[المائدة: 38]. وجه الاستدلال من النصين الكريمين: إن الله تعالى استخدم لفظ الجزاء بمعنى المقابل الذي لا يتخلّف عن الفعل.
3. وقد بنى بعض الفقهاء، وعلى رأسهم فقهاء الشافعية بعضاً من تخريجاتهم الفقهية على هذا الفهم، فقرروا في مسألة تعدد الجرائم والعقوبات ضرورة توقيع جميع العقوبات المحكوم بها على الجاني مهما تعددت باعتبار أن كل عقوبة تقابل فعلاً قد ارتكبه الجاني، وهذا بخلاف رأي من قال من الفقهاء بتداخل العقوبات التي هي من جنس واحد (الشيرازي (1959)، ص: 288).

4. ما روي في شأن المرأة المخزومية التي سرقت عقب فتح مكة، وقد اهتمت قريش لأمرها، وخافوا من تطبيق الحد عليها، فطلبوا من أسامة بن زيد –رضي الله عنهما- أن يشفع لها عند النبي، فلمّا فعل، غضب النبي ﷺ غضباً شديداً، وخطب الناس، فقال: «يا أيها الناس، إنما أهلك من كان قبلكم، أنهم كانوا إذا سرق فيهم الشريف تركوه، وإذا سرق فيهم الضعيف أقاموا عليه الحد، وأيم الله لو أن فاطمة بنت محمد سرقت لقطعت يدها» (البخاري، (بدون تاريخ) كتاب المغازي رقم (4053)، وأخرجه مسلم (2011)، في صحيح مسلم، كتاب الحدود رقم (3196).

وجه الدلالة من الحديث الشريف: أن الرسول الكريم ﷺ يشدد على تطبيق عقوبة الحد على كل من ثبت عليه قضاءً أنه ارتكب الجريمة المقرر لها تلك العقوبة، وأنه لا يجوز تعديلها أو إسقاطها والعفو عنها

5. تطبيق النبي ﷺ حد القذف على الذين قذفوا السيدة عائشة - رضي الله عنها- (سنن أبي داود، كتاب الحدود، حديث رقم (4474)).

6. وجه الدلالة من الواقعة فهم الفقهاء من هذه الواقعة اطراد مبدأ المساواة في تطبيق عقوبات الجرائم الحدية، يقول السهيلي في شرحه على سيرة ابن هشام عند ذكر توقيع الرسول ﷺ عقوبة الحد على القذفة: «وفيه التسوية بين أفضل الناس بعد النبي ﷺ وأدنى الناس درجة في الإيمان، لا يزاد القاذف على الثمانين وإن شتم خير الناس بعد رسول الله ﷺ ولا ينقص منها» (السهيلي (1967)، الجزء الثاني، ص:225).

ثانياً: هدف العقوبة منع الجريمة:

فالعقوبة في جزء من أهدافها -ولعله في الفقه الجنائي الإسلامي هو الهدف الأهم- ترمي إلى منع ارتكاب مزيد من الجرائم بما يحققه توقيع العقوبة على جريمة وقعت فعلاً من ردع عام وخاص (الماوردي، ص:293، وابن فرحون، (الجزء الثاني، ص:205)، والعوا (1983)، ص: 73)

ومما يدلل على ذلك أن أغلب الفقهاء كانوا يعرّفون العقوبة بما يُفهم منه صراحة مسألة الزجر والردع، فالماوردي الشافعي يعرّف الجريمة بأنها: «زواجر وضعها الله تعالى للردع عن ارتكاب ما حظر وترك ما أمر»، ويقرر الإمام القرافي المالكي - أن الزواجر مشروعة لدرء المفاسد المتوقعة، وأنها في معظمها زجراً للعصاة عن المعصية، وزجراً لمن يقدم بعدهم على المعصية (القرافي (1346)، ص:213).

كما قرر الكمال ابن الهمام في كتابه فتح القدير أن العقوبات في الفقه الجنائي

الإسلامي إنما شرعت لتحقيق الردع العام، ففي تنفيذها على المجرم منع له من العود للإجرام مرة أخرى، وفي تنفيذ العقوبة علناً أمام الناس ما يحقـــق المنع العام (ابن الهمام، ص:112)

ثالثاً: هدف العقوبة إصلاح الجاني:

مما لا شك فيه أن إصلاح الجاني كان من ضمن الأهداف التي تسعى العقوبات الشرعية إلى تحقيقها، إلا أن هذا الهدف كان أحياناً يتصدر أهداف العقوبة جميعها، وأحياناً أخرى نرى الأهداف الأخرى كالردع والزجر مثلاً هي التي تتصدر المشهد، وما ذاك إلا بسبب الموازنة الدقيقة التي تفرضها الشريعة الإسلامية لحفظ مصالح المجتمع من جهة وحفظ مصلحة الفرد من جهة أخرى (التميمي (2016) ، ص:127)

ولمّا كانت العقوبات الحديّة قد فرضت في مقابلة جرائم خطيرة تمس المجتمع وأمنه واستقراره، وفيها اعتداء على ضرورياته ومقومات وجوده، كان من الأجدى إنزال العقوبة الرادعة بالجاني، ذلك أنه أنزل الأذى بالأمة كلها، وبالتالي لا بد عند تقدير العقوبة من ملاحظة مقدار الأذى الذي أحدثه الجاني بالمجني عليه، إضافة إلى مدى الترويع والإفزاع العام الذي أحدثته الجريمة (أبو زهرة، ص:18)، فلا تقاس جريمة السرقة مثلاً - بمقدار المال المسروق، وإنما بما أحدثته هذه الجريمة من إخلال بضرورة من ضرورات حياة المجتمع وهي حفظ أموال الناس، وكذا القاتل بجريمته معتد على حق الحياة لكل نفس، يقول تعالى: ﴿مِنْ أَجْلِ ذَلِكَ كَتَبْنَا عَلَى بَنِي إِسْرَائِيلَ أَنَّهُ مَن قَتَلَ نَفْسًا بِغَيْرِ نَفْسٍ أَوْ فَسَادٍ فِي الْأَرْضِ فَكَأَنَّمَا قَتَلَ النَّاسَ جَمِيعًا وَمَنْ أَحْيَاهَا فَكَأَنَّمَا أَحْيَا النَّاسَ جَمِيعًا وَلَقَدْ جَاءَتْهُمْ رُسُلُنَا بِالْبَيِّنَاتِ ثُمَّ إِنَّ كَثِيرًا مِّنْهُم بَعْدَ ذَلِكَ فِي الْأَرْضِ لَمُسْرِفُونَ﴾[المائدة: 32]، لهذا كان القصاص رغم ما فيه من إتلاف للنفوس إلا أنه بمثابة الحياة للمجتمع، يقول تعالى: ﴿وَلَكُمْ فِي الْقِصَاصِ حَيَاةٌ يَا أُولِي الْأَلْبَابِ لَعَلَّكُمْ تَتَّقُونَ﴾[البقرة: 179]

وفي هذا المعنى يقول العز بن عبد السلام: «ربما كانت أسباب المصالح مفاسد، فيؤمر بها أو تباح، لا لكونها مفاسد، بل لكونها مؤدية إلى المصالح، وذلك كقطع الأيدي المتآكلة حفظاً للأرواح، والمخاطرة بالأرواح في الجهاد، وكذلك العقوبات الشرعية كلها ليست مطلوبة لكونها مفاسد، بل لكون المصلحة هي المقصود من شرعها، كقطع يد السارق وقاطع الطريق، وقتل الجناة ورجم الزناة ...» (العز بن عبد السلام (2003)، ص: 12)

وتأسيساً على العرض السابق لأهداف العقوبة الحديّة فإننا نقول: إن الشريعة الإسلامية بهذه الفلسفة لا تقر التفريد القضائي في مجال العقوبات الحديّة المقدرة، ولذلك فالفقهاء يقررون أن العقوبات الحديّة لا ينظر فيها إلى مقادير الأفعال الجرمية[3]، بقدر

ما ينظر فيها إلى مقدار انتهاكها لحرمات الله تعالى التي تحمي الفضيلة وتدفع الرذيلة، لذلك من سرق القليل عقوبته كمن سرق الكثير، ومن زنى بأمة كان في عقوبته كمن زنى بحرة، ومن قذف رجلاً من عامة الناس كان كمن قذف رجلاً من أشراف الناس (أبو زهرة، ص: 20)

وهنا يمكن أن يثار السؤال الآتي وهو: أليس في استبعاد مبدأ التفريد القضائي في العقوبات الحدية المقدرة قصور يجعل من الشريعة الإسلامية غير متوافقة مع هذه الحُقبة التي تطبق فيه الدراسات الاجتماعية والقانونية الحديثة الساعية لتحقيق الهدف الأول للعقوبة وهو إصلاح الجاني وليس معاقبته؟

وإجابة عن هذا التساؤل، عند دراسة الجرائم الحدية وعقوباتها في الشريعة الإسلامية يتضح بأن السياسة الجنائية الإسلامية تتسم بالتشدد تجاه عدد قليل جداً من الجرائم الماسة بأمن المجتمع ونظامه العام، حيث تُقدم مصلحة الجماعة على مصلحة الفرد، ويعود هذا هو السبب من تشدد الشارع الحكيم ووقف التفريد القضائي في العقوبات الحدية وعقوبة القصاص والدية، لأنها لو تركت للسلطة التشريعية والسلطة القضائية لتهاونوا في تقدير العقوبة لعدم إدراكهم مدى خطورة هذه الجرائم، وهذا ما يؤكده الواقع في القوانين الوضعية حيث استهانة بهذه الجرائم، فمن أجل ذلك وسداً لذريعة هذا الفساد جعل الشارع الكريم الجرائم الحدية بمعزل عن التفريد القضائي، فلا يجوز للقاضي إسقاط الحد، أو إبراؤه، أو الصلح معه أو العفو عنه، وإن ترتب على ذلك بعض المفاسد، كون المصلحة المترتبة على التشدد في عقوبات هذه الجرائم أعظم وأرجح من تلك المفاسد المشار إليها، فلا أهمية ولا عبرة لشخصية المجرم في مقابل فقدان أمن الجماعة وترويعهم بسبب وقوع تلك الجريمة، فالشارع يوائم بين مصلحة الجماعة ومصلحة الفرد، فإذا تعارضتا قدمت مصلحة الجماعة (التميمي (2016)، ص: 128).

وللتخفيف من ذلك الفساد ما أمكن تشدّدت السياسة الجنائية الإسلامية في إثبات هذه الجرائم بحيث يجعل من إثباتها أمراً في غاية الصعوبة، كما أمر بإسقاط العقوبة الحدية لمجرّد الشبهة، كما حث الشارع الحكيم على مسألة التوبة والستر قبل أن يصل الأمر إلى القضاء، إضافة إلى ما قررته الشريعة من الأحكام والبدائل التي تحول دون ارتكاب هذه الجرائم، فإن أصر المجرم بعد ذلك على هتك الحجب، واختراق الحواجز التي تحول بينه وبين ارتكاب جريمته، فإن مقتضى العدل وحفظ النظام العام للأمة يحتم أن يجازى المسيء بإساءته، ويكون الجزاء مناسباً لمقدار الأذى والضرر الذي ألحقه الجاني بالمجتمع من جراء ارتكابه لهذه الجريمة الخطيرة، وقد أسلفنا قبل قليل أن الفقهاء يقررون أن العقوبات

الحديّة لا ينظر فيها إلى مقادير الأفعال الجرمية، بقدر ما ينظر فيها إلى مقدار انتهاكها لحرمات الله تعالى - التي تحمى الفضيلة وتدفع الرذيلة، فالسارق يروّع الحي الذي نزلت الجريمة بساحته، والزاني يفسد الصلات بين الرجل والمرأة، فتكون العلاقات الآثمة، وبذلك تضيع الأنساب، والقاذف يشيع الفاحشة في الذين آمنوا ... وهكذا (التميمي (2016) مرجع سابق).

وبالإضافة إلى ذلك، فإن تشدد الشارع في الشروط الشرعية الواجب توافرها لإثبات الجرائم الحدية وجرائم القصاص والديه يجعل من تطبيق عقوباتها أمراً مستحيلاً، كسرقة ما لا قطع فيه، وهنا تكون هذه الجرائم تعزيزاً في مجال الحدود والقصاص، ويعمل القاضي مبدأ التفريد القضائي واختيار العقوبة الملائمة للمجرم والجريمة.

وإيقاع العقاب بالجاني هو مقتضى العدل، وهو لا ينافي الرحمة التي جاءت بها الشرائع السماوية، لذلك قرر النبي ﷺ فيما قرر من قوانين الرحمة -أن من لا يرحم الناس لا يرحمه القانون الرادع الزاجر(أبو زهرة، ص: 7)، فقال ﷺ: «من لا يرحم لا يُرحم» (صحيح مسلم، رقم: 4282)

يقول الإمام محمد أبو زهرة -رحمه الله-: «إن شذّاب المجتمعات كالناتئ من الأبنية، لا بد كي يكون النسق رائعاً وجميلاً وقوياً موثّق الأركان من أخذ هذا الناتئ بالمعول لتقوم عمد البناء، كالأشجار المثمرة لا تثمر إلا إذا شذّبت أطرافها من كل ما يتعلق بها من طفيل النبات» (أبو زهرة، ص: 7)

الفرع الثاني

فلسفة العقاب في الجرائم التعزيرية، وأثر ذلك على التفريد القضائي [4]

من خلال استقراء الكثير من الجرائم التعزيرية [5] نجد أن ردع الجناة وزجرهم هو هدف أصيل منشود لغايات استئصال الجريمة والحيلولة دون وقوعها ما أمكن، كما يظهر من تلك الوقائع المشار إليها أن ذلك لا يتم بمعزل عن النظر في شخصية الجاني والظروف التي أحاطت به عند ارتكابه للجريمة.

ولقد ظهر –أيضاً- أن من أهم الأسس التي يقوم عليها توقيع العقاب في هذا الجانب هو إصلاح الجاني نفسه من خلال اختيار العقوبة التي تناسب حالة بحيث يتحقق الردع والزجر المطلوب، وإلا صار توقيع العقوبة يتم بشكل آلي بمعزل عن المآلات التي قد تنجم عن ذلك ولو كانت هذه المآلات فاسدة، وبالتالي تفقد العقوبة هدفها المنشود وغاياتها المطلوبة، ويصير إيقاعها على الجاني نوعاً من أنواع التعسف في استخدام الحق (التميمي (2016)، ص: 129)

إن الوسيلة إذا غلب على الظن عدم إفضائها إلى الثمرة المرجوة منها لم تشرع، ذلك لأن استعمالها حينئذ يكون ضرباً من العبث أو الإضرار، وكلاهما لا يشرع لمناقضته قصد الشارع، يقول العز بن عبد السلام في كتابه القواعد: « كل تصرف تقاعد عن تحصيل مقصودة فهو باطل»(ابن عبد السلام (2003)، ص: 102)

ومن الأدلة والشواهد الدالة على التفريد القضائي في الجرائم التعزيرية ما يلي:

1. تشديد العقوبة لصفة خاصة في الفاعل (الجاني)، يقول تعالى: ﴿يَا نِسَاء النَّبِيِّ مَن يَأْتِ مِنكُنَّ بِفَاحِشَةٍ مُّبَيِّنَةٍ يُضَاعَفْ لَهَا الْعَذَابُ ضِعْفَيْنِ وَكَانَ ذَلِكَ عَلَى اللَّهِ يَسِيرًا﴾[الأحزاب: 30]، ووجه الدلالة من الآية الكريمة إن الجريمة كما تتغلّظ عليها العقوبة باجتماع الموانع تتغلّظ العقوبة –أيضاً -باجتماع النعم، ولهذا هدد الله ﷻ نساء النبي ﷺ بضعف ما هدد به غيرهن من النساء.
2. قوله ﷺ: «أقيلوا ذوي الهيئات عثراتهم» وفي رواية «أقيلوا ذوي الهيئات عثراتهم إلا الحدود» (ورد الحديث في مسند أحمد (رقم 24946)، كما أخرجه أبو داود في سنن أبي داود، كتاب الحدود (رقم 4375).

يقول ابن القيم في تعليقه على هذا الحديث ومبيناً وجه الدلالة منه ما نصه: «والظاهر أنهم ذوو الأقدار بين الناس في الجاه والشرف والسؤدد، فإن الله تعالى خصّهم بنوع تكريم وتفضيل على بني جنسهم، فمن كان منهم مستوراً، مشهوراً بالخير، حتى كبا به جواده، ونبا عضب صبره، وأديل عليه غلبة شيطانه، فلا يسارَع إلى تأديبه وعقوبته، بل تقال عثرته، ما لم تكن حداً من حدود الله تعالى، فإنه يتعين استيفاؤه من الشريف كما يتعين أخذه من الوضيع، فإن النبي ﷺ قال: «لو أن فاطمة بنت محمد سرقت لقطعت يدها»، وقال: «إن بني إسرائيل كان إذا سرق فيهم الشريف تركوه، وإذا سرق فيهم الضعيف قطعوه»، وهذا باب عظيم من أبواب محاسن هذه الشريعة الكاملة، وسياستها للعالم، وانتظامها لمصالح العباد في المعاش والمعاد» (ابن القيم (619-751)، ص: 171).

3. تقرر في كتب الفقه أن حبس المدين المماطل الممتنع عن الأداء شرع وسيلة لدفعه إلى إظهار ماله ليؤدي الدين الذي عليه، وذلك إذا غلب على الظن يساره، فيحبس بناء على طلب الدائن، فإذا ثبت

إعساره، فلا يجاب طلب الدائن حبسه، لأن في حبسه مجرد الإضرار الذي لا يؤدي إلى الغاية المنشودة. يقول العز بن عبد السلام في هذا الصدد: «إن ثبت إعساره فلا يجوز حبسه حتى يثبت يساره» (العز بن عبد السلام (2003)، ص: 103).

ويستدل من هذا الفقه أن الوسائل وإن كانت في أصلها مشروعة إلا أنها تسقط بسقوط مقاصدها، فإن علمنا أن حال الجاني لا ينصلح بالعقوبة المراد إيقاعها صار توقيعها عليه فقط - لمجرد الإضرار الذي لا يحقق الغاية المنشودة من العقاب وهي الردع والزجر والإصلاح (الرديني (1988)، ص: 254)

4. تشديد العقوبة في حالات العود، فمن المقرر في الشريعة أن من اعتاد الإجرام واستمراه فإنه يشدد عليه في العقوبة فإن لم يرتدع أمكن استئصاله من الجماعة بقتله أو بكف شره عنها بتخليده في الحبس، فمثلاً اللواطة لغير المحصن، يعاقب عليها الفاعل والمفعول به بالعقوبة المقررة للجريمة، فإن اعتاد الجناة هذه الجريمة ولم تردعهم العقوبة أمكن قتلهم لشناعة جرمهم وأثره الخطير على أمن المجتمع وسلامة أخلاقه، كما أن السارق إذا لم تردعه العقوبة، وعاد إلى الجريمة مرة بعد مرة أمكن تخليده في الحبس حتى يموت أو تظهر توبته (عوده (2020)، ص: 768).

5. ما روي من فتوى إمام الأندلس يحيى بن يحيى الليثي صاحب مالك لبعض ملوك المغاربة وهو الأمير عبد الرحمن بن الحكم الأموي صاحب الأندلس، وكان قد نظر في رمضان إلى جارية له كان يحبها حباً شديداً، فعبث بها، فلم يملك نفسه أن وقع عليها، ثم ندم ندماً شديداً، فسأل الفقهاء عن توبته وكفارته، فقال يحيى بن يحيى: تصوم شهرين متتابعين، فلمّا بدر يحيى بذلك سكت بقية الفقهاء حتى خرجوا، فقالوا ليحيى: مالك لم تفته بمذهب مالك، وهو التخيير بين العتق والصيام والإطعام؟ فقال: لو فتحنا له هذا الباب سهل عليه أن يطأ كل يوم ويعتق رقبة، ولكن حملته على أصعب الأمور لئلا يعود (المرداوي(2002)، ص: 3407).

ورغم إنكار بعض الفقهاء كالغزالي والجويني لهذه الفتوى بدعوى مخالفتها للنصوص، إلا أن البعض الآخر من الفقهاء من أيّد هذه الفتوى وانتصر لها، يقول الإمام يحيى الطوفي الحنبلي: «أمّا تعين الصوم في كفارة رمضان على الموسر، فليس يبعد إذا أدى إليه اجتهاد مجتهد، وليس ذلك من باب وضع الشرع بالرأي، بل من باب الاجتهاد بالمصلحة، أو من باب تخصيص العام المستفاد من ترك الاستفصال في حديث الأعرابي (الحديث رواه أبو هريرة أن رجلاً جاء إلى النبي ﷺ قال: هلكت، قال: ما شأنك؟ قال: وقعت على امرأتي في رمضان، قال: هل تجد ما تعتق

رقبة؟ قال: لا، قال: فهل تستطيع أن تصوم شهرين متتابعين؟ قال: لا، قال: فهل تستطيع أن تطعم ستين مسكيناً؟ قال: لا أجد، فأتى النبي ﷺ بعرق فيه تمر، فقال: خذ هذا فتصدق به، فقال أعلى أفقر منا؟ ثم قال: خذه فأطعمه أهلك. أخرجه البخاري في صحيحه، كتاب الصوم، تحت رقم (1834))، وهو عام ضعيف، فيخص بهذا الاجتهاد المصلحي المناسب، وقد فرّق الشرع بين الغني والفقير في كثير من المواضع، فليكن هذا من تلك المواضع» (المرداوي (2002)، ص: 3407)

ولقد علّق القرافي على هذه الفتوى بما أورده صاحب الفواكه بما معناه: «إن الكفّارات شرعت للزجر والملوك لا تنزجر بالإعتاق، لسهولته عليهم، فتعيّن ما هو زاجر لهم، وهذا من النظر في المصلحة، ولا تأباه القواعد، ولعله غير مناف للتخيير، لإمكان حمل التخيير على فقد المعّين لنوع منها» (النفراوي (1995)، ص: 315)

وقال القرافي في تهذيب الفروق: «إفتاء يحيى له بالصوم هو الأوفق بكون مشروعية الكفّارات للزجر، ولم يفته يحيى على أنه أمر لا يجوز غيره».

6. ورد في كتب الفقه الحنفي عن (الكاساني (1982)، ص: 64) والزيلعي، ص: 634، والصنعاني، ص: 54) أن الفقهاء كانوا يقسّمون الناس -عند ارتكابهم للجرائم التعزيرية- إلى أربع مراتب، وهي على النحو الآتي:

المرتبة الأولى: وهم أشراف الناس من العلماء والفقهاء والأتقياء الذين عرفوا بالصلاح وهم سادة الناس يتبعونهم ويأخذون بآرائهم، فلو بدر من واحد من هؤلاء زلة ليست له عادة، أرسل إليه القاضي أمينه يقول له: بلغني أنك فعلت كذا وكذا. وفي هذا أبلغ الأثر في نفوس أصحاب هذه المرتبة.

المرتبة الثانية: الأشراف من الأمراء والقادة ووجهاء الناس، ويكون تعزيرهم باستدعائهم إلى مجلس القضاء وإعلامهم بما بدر منهم ومواجهتهم بذلك، ولذلك وقعه الكبير في نفوس هؤلاء لما يحمله ذلك من الزجر.

المرتبة الثالثة: أوساط الناس وهم غالبية المجتمع وعامته، فإن بدر من هؤلاء شيء مما يستوجب التعزير جُلبُوا بواسطة الشرطة إلى مجلس القضاء، وعوقبوا بما يصلح حالهم، سواء أكان ذلك بالحبس أم بغيره.

المرتبة الرابعة: الأخسّاء وهم سفلة الناس ممن اشتهروا بسوء الخلق وقلة الأدب واعتادوا الإساءة، فهؤلاء يقادون إلى المحاكم ويعنّفوا، وربما يضربون ثم يتم إيقاع العقوبة المناسبة بحقهم.

ونلحظ من هذه التقسيمات السالفة أن شخصية المجرم وسلوكياته وأسبقياته والظروف المحيطة به لها أثر بالغ في تحديد العقوبة المناسبة في الجرائم التعزيرية يقول القرافي: «إن التعزير يختلف باختلاف الأعمار والأمصار، فرب تعزير في بلد يكون إكراماً في بلد آخر، كقطع الطيلسان (يُذكر أن الطيلسان من ألبسة العجم (الفيومي، دون تاريخ) ليس تعزيراً في الشام فإنه إكرام، وكشف الرأس عند الأندلسيين ليس هواناً وبمصر والعراق هوان» (هذه الأدلة لا يمكننا إلا أن نقول: إن ما يسمى بـ (التفريد القضائي) هو مصطلح مشروع في أصله في الفقه الجنائي الإسلامي ويتجلى ظهوره في الجرائم التعزيرية التي تشكل غالب الوقائع الجرمية التي تحدث في المجتمع.

المطلب الثاني

- **مفهوم التفريد القضائي في الفقه الوضعي**

التفريد القضائي هو مصطلح نتج عن تطور الفلسفة الكامنة وراء تشريع العقاب في القوانين الجنائية المعاصرة، فهو جزء من سياسة العقاب المعاصرة «تفريد العقاب»، أي ملائمة العقوبة للفرد، والتي تمر بثلاثة مستويات أولهما التفريد التشريعي بواسطة تحديد المشرع عقوبات للجريمة وفقاً لجسامتها وظروف فاعلها (سرور (1972) ، ص: (245) وإبراهيم (2011) ص: (11))، كأن يحدد عقوبة ذات حد أدنى وحد أقصى، وكذلك تقدير الظروف المشددة، سواء أكانت ظروفا مادية مثل استخدام المادة السامة في القتل، أو ظروفا شخصية مثل سبق الإصرار في جريمة القتل (السيد (2003)، ص: 23 وما بعدها)، وكذلك من مظاهر التفريد التشريعي تبني المشرع لنظام الأعذار القانونية المعفية والمخففة من العقوبة، وقانون خاص للأحداث الجانحين.

وتفريد قضائي تختص به السلطة القضائية، وتفريد تنفيذي تختص به المنشآت العقابية والإصلاحية القائمة على تنفيذ العقوبة، ويكون عن طريق إخضاع المحكومين لبرامج إصلاح وإعادة التأهيل المعدة وفقاً لشخصياتهم، بعد فحصهم طبياً وتشخيص حالتهم البيولوجية والنفسية والاجتماعية، وبناءً على نتيجة الفحص يخضع المحكوم لما يلائمه من المعاملة في المؤسسة العقابية والإصلاحية وبذلك يتحقق التفريد التنفيذي للعقاب (الجوهري (2002)، ص: 6)، ومن صور التفريد التنفيذي، العقوبة غير محددة المدة، وجواز الإفراج الشرطي عن المحكوم عليه إذا استوفى مدة معينة من العقوبة المحكوم بها عليه و وجد ما يدعو إلى الثقة بأنه لن يعود إلى سلوك طريق الجريمة مرة أخرى (إبراهيم (2011)، ص 196).

ومن المعلوم أن النصوص القانونية التي يقرها المشرع لوسائل التفريد تأتي عامة ومجردة، فهي بعيدة عن الواقع الذي لا يمكن أن يلمسهُ إلا القاضي الجنائي، فهو الذي يحيط بكل الوقائع والظروف والملابسات التي تحيط بالجريمة والمجرم، وهو الذي يقدر طبيعة شخص الجاني ودرجة خطورته ومدى قابليته للإصلاح والتهذيب والتقويم، لذلك فإن تحقيق مقصد الشارع من العقاب هي قضية القاضي الجنائي الذي يملك سلطة تقديرية في وزن العقوبة بالنسبة إلى الجريمة والمجرم، وللتعرف على مفهوم التفريد القضائي، يقتضي بيان التعريف الفقهي للتفريد القضائي، وتعريف القضاء، ولذلك قسمنا هذا المطلب إلى فرعين على النحو الآتي

الفرع الأول

- **التعريف الفقهي للتفريد القضائي**

يُقصد بالتفريد القضائي تطبيق السلطة القضائية للعقوبة بواسطة إخضاع كل جانٍ لما يلائمه من عقوبة أو تدبير علاجي أو وقائي يتناسب مع شخصيته وخطورته الإجرامية لغايات الإصلاح والتقويم والتهذيب (راشد (1964)، ص:215 ومعايدة (2009)، ص:23)، ومن صور هذا التفريد أن يترك المشرع للقاضي الخيار بين عقوبتين كالحبس أو الغرامة، أول حكم بالعقوبة الأصلية مع النفاذ، أو إيقاف تنفيذ العقوبة إذا توافرت شروطه.

ويشترط أن يتناسب العقاب مع النتيجة الإجرامية لكل جريمة، فيأخذ بعيّن الاعتبار الظروف والدوافع والفروقات الشخصية التي تدفع كل جانٍ إلى ارتكاب جريمته، سواء أكانت داخلية أو خارجية، فلا يكون العقاب عاماً موحداً (أبوزيد، ص: 303).

ويرى جانب من الفقه بأنها سلطة تقديرية واسعة تعطى للقاضي لاختيار العقوبة المناسبة من حيث الكم والنوع والمقدار للحالة الماثلة أمامه (الجبور (2009) ص: 23)

وفي سبيل تحقيق تلك الغاية يعمد المشرّع إلى تحديد العقوبة تحديداً مادياً متناسباً مع مادياتها، ولذلك فهو لا يستطيع أن يحقق التناسب بين العقوبة وشخصية كل من يرتكب الجريمة لانعدام علمه وقت التجريم والعقاب (حمودة، (2021) ص 270).

ورغم الجسامة الذاتية للجريمة الواحدة أيا كان سبب وقوعها وزمانها، إلا أن المشرع بعد أن يقدر جسامتها في صورة حد أقصى وحد أدنى للعقاب (الجوهري، (2002) ص 3) ، يترك للقاضي أن يكمل هذا التحديد التشريعي للعقوبة بوصوله إلى التحديد الواقعي للعقوبة عن طريق إدخال التحديد التشريعي المجرد للعقوبة في إطار التحديد الذي يراعي فيه القاضي شخصية مرتكب الجريمة، بحيث تكون العقوبة المحكوم بها متناسبة مع

الجريمة ومع درجة إثم وظروف مرتكبها (حمودة، (2021) ص 270-271) ، ومن هنا تبدو أهمية التفريد القضائي في تحقيق مقصد الشارع من العقاب عن طريق تطبيق النصوص التشريعية على الحالات الواقعية، لهذا تأتي النصوص القانونية التي تسمح بالتفريد مرنة وواسعة تمكن القاضي من أعمال سلطته التقديرية في حدود معينة وضوابط محددة الهدف منها ضمان سلامة الحكم وتحقيق وظائف العقاب في إطار العدالة والمساواة

الفرع الثاني

- **التعريف القضائي للتفريد**

أشارت المحكمة الاتحادية العليا (2016) في الطعن رقم 366-329 لسنة 2015 – جزائي خلال جلستها بتاريخ 04/01/2016 إلى « أن تقدير العقوبة في الحدود المقررة قانونا وتقدير قيام موجبات الرأفة من عدم قيامها من إطلاقات محكمة الموضوع دون معقب، ودون أن تسأل حسابًا عن الأسباب التي من أجلها أوقعت العقوبة بالقدر الذي ارتأته ما دام تقدر التزمت بحدود العقوبة في القانون، وكان ضمن الحد الأدنى والأقصى المقرين في القانون».

وقررت ذات المحكمة في تطبيق العقوبة بأنه « تقدير الظروف المخففة أو استعمال الرأفة من صلاحيات محكمة الموضوع لا تخضع فيها لرقابة المحكمة العليا في تقدير العقوبة متى جاءت في حدود ما نص عليه القانون مثال في حيازة وتعاطي مواد مخدرة عوقب فيها المتهم بالحد الأدنى للعقوبة مستعملا سلطته في تقدير العقوبة (في حكم الطعن رقم 155 لسنة 23 شرعي، المحكمة الاتحادية العليا (2002) في جلستها بتاريخ 2002/11/09.

المبحث الثاني

- **التفريد التشريعي وفقاً لما نص عليه المرسوم، وعلى ضوء سلطة القاضي الجنائي التقديرية في تطبيقه**

سأتناول في هذا المبحث أنواع تفريد العقوبة في قانون دخول وإقامة الأجانب لدولة الإمارات العربية المتحدة، ووفقاً لما نص عليه المرسوم بقانون اتحادي رقم (29) لسنة 2021، وإغناء البحث فيه يقتضي توزيعه على مطلبين، أُفرد الأول: للتفريد التشريعي في المرسوم كأساس قانوني للتفريد القضائي، وأخصص الثاني: للتفريد القضائي وفقاً لسلطة القاضي الجنائي في تطبيقه للمرسوم.

المطلب الأول

- **التفريد التشريعي في المرسوم كأساس قانوني للتفريد القضائي**

التفريد التشريعي هو سن المشرع الإماراتي قانوناً ذات حدين أعلى وأدنى، مراعياً فيه الظروف الشخصية للمجرم قاصداً تقويمه وتأهيله، والخطورة المادية للجريمة، بناءً على خبراته وتنبؤاته وقت وضع نصوص التجريم والعقاب

وبالنظر في العقوبات الواردة في المرسوم بقانون اتحادي رقم (29) لسنة 2021، في شأن دخول وإقامة الأجانب نجد بأن المشرع الإماراتي نص على عقوبة الحبس في المادة (21) لكل أجنبي يضبط في الدولة بعد أن تسلل أو دخلها بصورة غير مشروعة، وعلى المحكمة أن تأمر بإبعاد الأجنبي ومصادرة الأموال التي تحصل عليها الأجنبي من أي نشاط أو عمل قام به خلال هذه المدة

ونصت المادة (70) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 من قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة على أن الحبس هو وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة لهذا الغرض لمدة لا تقل عن شهر ولا تزيد عن ثلاث سنوات ما لم ينص القانون خلاف ذلك

وعاقب بالسجن المؤقت قائد أي وسيلة من وسائل النقل إذا أدخل أو أخرج أو حاول إدخال أو إخراج أجنبي للدولة بالمخالفة لأحكام هذا المرسوم بقانون في الفقرة (1) من المادة (21)، وعاقب بذات العقوبة الواردة في البند السابق كل من أرشد أو حاول أو دل أو ساعد بأي صورة من صور المساعدة متسللاً للوصول إلى داخل الدولة أو الخروج منها، في الفقرة (2) من ذات المادة.

والسجن المؤقت هو وضع المحكوم عليه في إحدى المنشآت العقابية المخصصة لهذا الغرض لمدة لا تقل عن (3) ثلاث سنوات، ولا تزيد على (15) خمس عشرة سنة ما لم ينص القانون خلاف ذلك ([6]).

ونص في المادة (23) من ذات المرسوم على عقوبة الحبس لمدة لا تزيد على (6) أشهر، وبالغرامة التي لا تقل عن (5000) خمسة آلاف درهم ولا تزيد على (10.000) عشرة آلاف درهم أو بإحدى هاتين العقوبتين كل من أعطى بياناً كاذباً بقصد التهرب من أحكام هذا المرسوم بقانون، وللمحكمة أن تأمر بإبعاد الأجنبي عن الدولة.

وعاقب في المادة (24) بالسجن مدة لا تزيد على (10) عشر سنوات كل من زوّر تأشيرةً أو تصريحاً بالإقامة أو أي محرر رسمي تصدر بناءً عليها هذه التأشيرات أو التصاريح، وذلك بقصد التهرب من أحكام هذا المرسوم بقانون، وكل من استعمل أي مستند مزور من المستندات المشار إليها في هذه المادة مع علمه بتزويره.

ونص في المادة (25) على عقوبة الحبس مدة لا تقل عن شهرين وبغرامة مقدارها (100.000) مئة ألف درهم لكل من استخدم أو آوى متسللاً

ونصت المادة (26) على عقوبة الحبس مدة لا تزيد على (3) أشهر والغرامة التي لا تزيد على (10.000) عشرة آلاف درهم أو بإحدى هاتين العقوبتين، كل من خالف شروط وضوابط تصاريح الإقامة المشار إليها في المادة (8) من هذا المرسوم بقانون، وعلى المحكمة أن تأمر بإبعاد المخالف عن الدولة

ونصت المادة (27) على عقوبة الحبس أو الغرامة التي لا تقل عن (10.000) عشرة آلاف درهم، كل من استغل أو ساعد أو شارك أو سهل بأي وسيلة كانت، تأشيرة بشكل لا يتفق مع الغرض الذي منح من أجله بالمخالفة لأحكام هذا المرسوم بقانون ولائحته التنفيذية، وتتعدد العقوبات بتعدد المخالفين، وعلى المحكمة أن تأمر بإبعاد الأجنبي

ونصت المادة (29) على عقوبة الحبس مدة لا تزيد على (3) ثلاثة أشهر أو بالغرامة التي لا تزيد على (4.000) أربعة آلاف درهم، كل أجنبي تخلف عن سداد الغرامة المشار إليهما في المادتين (11) و (12) من ذات المرسوم بقانون، ويجوز للمحكمة أن تأمر بإبعاده

ونصت المادة (30) على عقوبة الحبس مدة لا تقل عن شهر والغرامة التي لا تقل عن (10.000) عشرة آلاف درهم، أو بإحدى هاتين العقوبتين كل من يخالف أحكام هذا المرسوم بقانون أو لائحته التنفيذية أو القرارات الصادرة تنفيذاً له، فيما عدا العقوبات المقررة للجرائم المنصوص عليه في هذا المرسوم بقانون، وتتعدد الغرامة بتعدد الأشخاص المخالفين

فبالنظر في سياسة المشرع الإماراتي في التجريم والعقاب في قانون دخول وإقامة الأجانب نجد بأنه جرم الأفعال التي قدر لها الحماية الجنائية، وقدَر لها عقوبات مختلفة تتناسب مع جسامة كل جريمة وظروفها، والخطورة الإجرامية للجاني وآثارها، وهذا ما يسمى بالتفريد التشريعي، ويعتبر الأساس القانوني للتفريد القضائي

المطلب الثاني

- **التفريد القضائي وفقاً لسلطة القاضي الجنائي التقديرية في تطبيقه**

سبق أن أوضحنا بأن التفريد التشريعي يعتبر بمثابة الأساس القانوني للتفريد القضائي، وهو بمثابة اعتراف من المشرع بالسلطة التقديرية للقاضي الجنائي لتمكينه من تفريد العقوبة وتحقيق مقصده من العقاب المتمثل في تحقيق مبادئ العدالة وإصلاح المحكوم عليه وإعادة دمجه في المجتمع، ووضع المشرع الإماراتي الضوابط التي تعين القاضي الجنائي في عملية التفريد القضائي للعقاب كما هو معمول به في الشريعة الإسلامية، وأخذت به التشريعات الوضعية تحت مصطلح « المعيار المزدوج»

ومن أساليب التفريد القضائي التي منحها مشرع دولة الإمارات العربية المتحدة للقاضي الجنائي في تطبيقه للمرسوم بقانون اتحادي رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب من أجل تحقيق أغراض المشرع من العقاب والمتمثلة في تحقيق الردع العام والردع الخاص وتحقيق العدالة للأفراد أما القانون نظام التدرج الكمي والنوعي للعقوبة، والأعذار القانونية والظروف التقديرية المخففة والمشددة، والتدابير الجنائية، والدفاع الاجتماعي، إلا أنه استثنى من ذلك كله وقف التنفيذ، واستبدال العقوبة، والعفو القضائي، الوارد في قانون العقوبات، وهذا ما نصت عليه المادة (32) من المرسوم بقانون اتحادي « في تطبيق العقوبات المنصوص عليها في المواد السابقة، لا تسري أحكام المواد الخاصة بوقف التنفيذ، واستبدال العقوبة، والعفو القضائي، الواردة في قانون العقوبات»

ومن هنا يثور التساؤل الرئيسي لمشكلة البحث، وهي ما أثر العمل بالتفريد القضائي وفقاً لما جاء به المشرع في المرسوم بقانون اتحادي – محل الدراسة- في تحقيق مقصده المشرع من العقاب؟

وبصياغة أخرى، ما أثر عدم العمل بوقف التنفيذ، واستبدال العقوبة، والعفو القضائي، في تحقيق مبادئ العدالة وإصلاح المحكوم عليهم وإعادة دمجهم في المجتمع، والمخاطبين بأحكام هذا القانون؟

وللإجابة عن هذا التساؤل نقول والله الموفق:

1. إن المتأمل في السياسة التشريعية الجنائية للمشرع في دولة الإمارات العربية المتحدة يجد أن مقصد الشارع من العقاب هو تحقيق أغراض العقوبة من الردع العام والردع الخاص وتحقيق العدالة، وأعطى المشرع السلطة القضائية الأدوات اللازمة لتفريد العقاب وتحقيق مقصده منه، وتحقيق العدالة والمساواة الفعلية بين المخاطبين بأحكام القاعدة القانونية ، وذلك من خلال النظام العقابي المرن المتمثل بنظام التدرج الكمي والنوعي للعقوبة، ووقف تنفيذ العقوبة، والأعذار القانونية والظروف التقديرية المخففة والمشددة، وأن يعين لكل جريمة عدة أنواع من العقوبات المحددة ليختار منها القاضي العقوبة الأكثر ملائمة لكل حالة منظورة أمامه، وعليه فإن حرمان القاضي لأحد هذه الأدوات يمكن أن يترتب عليه عدم تحقيق مقصد الشارع من العقاب والمتمثل في تحقيق مبادئ العدالة الجنائية والمساواة الفعلية بين المحكوم عليهم بحيث يلقى كل محكوم عليه العقوبة الملائمة لشخصيته.
2. أخذ المشرع الإماراتي بنظام وقف تنفيذ العقوبة في قانون العقوبات الاتحادي، كوسيلة للقاضي الجنائي يستطيع من خلالها وضع المحكوم عليه تحت التجربة والاختبار، إذا رأى من أخلاق المحكوم عليه أو ماضيه أو عمره أو الظروف التي ارتكب فيها الجريمة ما يبعث على الاعتقاد بأنه لن يعود إلى ارتكاب جريمة جديدة، وهذا ما عمل به سيدنا عمر بن الخطاب – رضي الله عنه- في عام الرمادة، عندما أوقف حد السرقة فيمن سرق بسبب الجوع، وهذا ذاته ما عملت به التشريعات الوضعية الحديثة كنظام يُمكن القاضي من تحقيق العدالة والمساواة من خلال تحقيق أفضل ملائمة بين ظروف الجاني وظروف جريمته من جهة، والعقوبة من جهة أخرى، وكذلك تجنبيه مساوئ الاختلاط بالمجرمين، وأنه من العدالة أن يفسح المجال لإعادة تأهيله خارج المؤسسات العقابية، حيث أثبتت العديد من الدراسات والتجارب أن العقوبات السالبة للحرية خصوصاً قصيرة المدة لها آثار سلبية على المحكوم عليه، وبصورة خاصة مجرم الصدفة أو المجرم العرضي، حيث إن احتكاكه بالمجرمين المعتادين في المؤسسات العقابية قد يؤدي إلى إفساده بدلاً من إصلاحه، الأمر الذي استوجب ضرورة البحث عن نظام بديل بعد أن ثبت عجز العقوبات السالبة للحرية في الحد من الظواهر الإجرامية وإصلاح وإعادة تأهيل المحكوم عليهم، وهو نظام وقف العقوبة، وعليه فإنه عدول المشرع عن هذه السياسة بنصه على عدم سريان أحكام المواد الخاصة بوقف التنفيذ، واستبدال العقوبة، والعفو القضائي، الواردة في قانون العقوبات يمكن من شأنه أن يحول دون تحقيق مقاصد العقاب.

3. المعالجة التشريعية للعقاب في مرحلة التشريع تتم بصورة عامة ومجردة، إذ يقدر المشرع جسامة العقوبة بالنظر إلى جسامة ماديات الجريمة، أو إثم مقترفها، أو إليها معاً، معتمداً في هذه الحالات على اعتبارات عامة تصدق على أغلب الأشخاص بصفاتهم وليس بذواتهم، ولا يكون في ذهنه شخص بذاته ولا واقعة معينة، وهنا يأتي دور التفريد القضائي في تطبيق العقوبة بهدف تكملة العمل التشريعي، وذلك باستخراج التحديد الواقعي للعقوبة من التحديد المجرد إلى التحديد الواقعي، والقاضي هو الذي يقدر هذه العناصر بمقتضى سلطته في مجال تفريد العقوبة، فالأصل في العقوبة هو تفريدها لا تعميمها، ولذا؛ فإن تقرير الخروج عن هذا الأصل أين كانت الأغراض التي يتوخاها المشرع من ذلك مؤداه التسليم بأن ظروف الجناة قد تماثلت بما يقتضي توحيد العقوبة التي توقع على كل متهم، وهو الأمر الذي تفقد معه العقوبة تناسبها مع ظروف الجريمة وملابساتها وسمات الجاني الشخصية.

4. التفريد الجزائي للعقوبة يتكون من عناصر وهي التفريد التشريعي، والتفريد القضائي، والتفريد التنفيذي، وكل عنصر من هذه العناصر له أدواته وأساليبه التي تستخدم لتحقيق أغراض العقوبة التي يتوخاها المشرع الإماراتي في قانون دخول وإقامة الأجانب – محل الدراسة- وعليه، فإن تقييد عنصر من هذه العناصر، أو أداة من أدواته أو أساليبه يعطل النتائج المرجوة، هذا بالإضافة إلى أننا لا نكون بصدد تفريد حقيقي أو تفريد كامل، لانعدام نوع من أنواعه، أو أداة من أدواته، وبناء عليه فإن الهدف المنشود من العقوبة وهو تحقيق العدالة الجنائية بواسطة ردع الجناة وزجرهم لغايات استئصال الجريمة والحيلولة دون وقوعها، مع مراعاة الظروف الشخصية للجاني والظروف التي أحاطت به عند ارتكاب الجريمة لن يتحقق.

النتائج والتوصيات

أولاً: النتائج:

1. مهّد لظهور مصطلح التفريد القضائي الكثير من الدراسات القانونية والأبحاث الاجتماعية والتي كانت تستهدف الجريمة والمجرم وكيفية استئصالها أو التقليل من ارتكابها بما يتلاءم مع شخصية المجرم.
2. عرف الفقه الجنائي الإسلامي مضامين مصطلح التفريد القضائي منذ قرون عديدة، وذلك بسبب تقسيم الشريعة الإسلامية الجرائم إلى جرائم حدية وجرائم تعزيرية والذي يعتبر نوع من أنواع التفريد الجزائي في شقه التشريعي والذي يتيح للقاضي ممارسة التفريد القضائي،

كما أن حصر الجرائم الحدية بهذا العد القليل واعتبار باقي الجرائم تعزيرية يعطي مؤشر ذو دلالة واضحة نحو التوسع في التفريد القضائي بما يحقق مقصد الشارع من العقاب.

3. التفريد القضائي الذي عرفته النظريات الحديثة للعقاب يتوافق مع ما جاءت به الشريعة الإسلامية من حيث إصلاح المتهم، وإن كانت الشريعة تتفوق على هذه النظريات في كونها قائمة على قواعد ومبادئ وكليات تعطيه القدرة الفائقة على استيعاب كافة الوسائل والآليات الشرعية التي تحقق مصلحة المجتمع.

ثانياً: التوصيات

يقترح الباحث تعديل نص المادة (32) من المرسوم بقانون رقم (29) لسنة 2021 في شأن دخول وإقامة الأجانب، بحيث يسمح للقاضي الجنائي بممارسة سلطته التقديرية في التفريد القضائي.

1. العقوبة لغة اسم مصدر من عاقب يعاقب معاقبة وعقابا، يقال: عاقبه بذنبه، أي: أخذه به، والعقاب والمعاقبة أي أن تجزي الرجل بما فعل سوءاً، ينظر لسان العرب ابن منظور، محمد بن منظور، بيروت، دار صادر، الطبعة الثالثة، 1414هـ، 1/ 619. وفي اصطلاح الفقه الإسلامي عرفت بأنها زواج وضعها الله تعالى للردع عن ارتكاب ما حظر، وترك ما أمر به»، الأحكام السلطانية، الماوردي، علي بن محمد الماوردي، القاهرة، دار الحديث، ص 325. وفي اصطلاح القانون الوضعي عرفت بأنها: « الجزاء الذي يقرره القانون، ويوقعه القاضي من أجل الجريمة ويتناسب معها» شرح قانون العقوبات القسم العام، حمودة، علي محمود، قانون العقوبات النظرية العامة للجزاء الجنائي، أكاديمية شرطة دبي، ط 1، الإمارات العربي المتحدة، ص 270.
2. الجرائم الحدية هي تلك الجرائم التي رتب الشارع لها عقوبة محددة، ولم يترك أمر تقدير العقوبات فيها إلى القاضي وذلك لخطورة هذه الجرائم على أمن المجتمع، ونظامه العام. انظر الماوردي، المرجع السابق.
3. نشير هنا إلى الخلاف الذي وقع بين العلماء في العقوبات المقررة لجريمة الحرابة، حيث وقع الخلاف بين العلماء في تلك العقوبات وهي القتل والصلب والتقطيع من خلاف والنفي، ذلك أن الله تعالى ذكرها في الآية الكريمة وفصل بينها بحرف «أو» فمنهم من رأى أن أو تفيد الترتيب وبالتالي فالقاضي عليه أن يحدد العقوبة بما يتناسب والجريمة المرتكبة فمن قتل يقتل ومن سرق يقطع. وهذا هو قول الجمهور من العلماء، وخالف مالك والظاهرية في المسألة وقالوا: إن هذه العقوبات ليست

على ترتيب الأفعال الجرمية وجسامتها، وإنما هي عقوبات يتخير منها القاضي ما يحقق الصلاح للجاني والمجتمع في الواقعة المعروضة عليه. انظر تفصيل المسألة في: مالك، المدونة الكبرى، مطبعة السعادة 1323هـ، ج16، ص298. ابن حزم، المحلى، دار الفكر، بيروت، ج11، ص317.

4. الجرائم التعزيرية: هي تلك الجرائم التي لم يرد نص من الشارع على عقوبة مقدرة لها، رغم ثبوت نهي الشارع عنها لكونها مفسدة أو تؤدي إلى مفسدة.

5. والجرائم التعزيرية: تستوعب الجل الأعظم من الوقائع الجرمية التي تقع في المجتمع، بحيث لا يستثنى من تلك الوقائع إلا الجرائم المقدرة عقوباتها من قبل الشارع وهي تعد على أصابع اليدين.

6. الإبراهيمي: (1432-2011)، أكرم نشأت، السياسة الجنائية دراسة مقارنة، دار الثقافة للطباعة والنشر.

7. ابن الهمام: الكمال، فتح القدير، دار الفكر، بيروت، الطبعة الثانية، الجزء الرابع.

8. ابن حزم: المحلى، دار الفكر، بيروت، الجزء الحادي عشر.

9. ابن عبد السلام، عز الدين، القواعد الكبرى، الجزء الأول.

10. ابن فارس (1979)، أحمد بن فارس، معجم مقاييس اللغة، تحقيق: عبد السلام محمد هارون، بيروت، دار الفكر.

11. ابن فرحون، تبصرة الحكام في أصول الأقضية ومناهج الأحكام، الطبعة الأولى، دار الكتب العلمية، بيروت، لبنان.

12. ابن منظور (1414هـ)، محمد بن منظور، لسان العرب، بيروت، دار صادر، الطبعة الثالثة.

13. أبو داود، سليمان. سنن أبي داود، كتاب الحدود، حديث رقم (4474).

14. أبو زهرة، محمد، الجريمة والعقوبة.

15. الأزهري (2001)، محمد بن أحمد. تهذيب اللغة، تحقيق: محمد عوض مرعب، بيروت، دار إحياء التراث العربي.

16. البخاري، محمد بن إسماعيل. الجامع الصحيح، كتاب المغازي تحت رقم (4053)، دار الكتب العلمية، بيروت.

17. الجوهري (2002)، مصطفى فهمي. تفريد العقوبة في القانون الجنائي: دراسة تحليلية تأصيلية في القانون المصري وقوانين بعض الدول العربية، دار النهضة العربية، القاهرة.

18. جيرمي بنتام، الموسوعة العربية، المجلد الخامس، العلوم القانونية والاقتصادية.

19. حسني (1972)، محمود نجيب، علم العقاب، دار النهضة العربية.

20. الدريني (1988)، فتحي، نظرية التعسف في استعمال الحق، مؤسسة الرسالة.

21. راشد (1964)، علي، ورقة مقدمة لمجموعة أعمال الحلقة العربية للدفاع الاجتماعي، القاهرة.

22. الروسان، إيهاب، التفريد القضائي للعقوبة، دار المسيرة، الطبعة الأولى، عمان، الأردن.

23. الزحيلي، وهبه بن مصطفى. الفقه الإسلامي وأدلته، دمشق، دار الفكر، الطبعة الرابعة، د.ت، 5343/7.

24. الزيلعي، تبيين الحقائق، المطبعة الأميرية، القاهرة.

25. سرور (1972)، أحمد فتحي، أصول السياسة الجنائية، دار النهضة العربية.

26. سلامة (1975)، مأمون محمد، حدود سلطة القاضي الجنائية في تطبيق القانون، دار الفكر العربي.

27. السهيلي (1967)، عبد الرحمن. الروض الأنف، دار الكتب الإسلامية.

28. شهاب الدين أحمد بن إدريس المصري المالكي (643-723)، القرافي، الفروق.

بحث بعنوان:

استدامة ريادة الخدمات
دراسة تطبيقية على الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ في دولة الإمارات

د. سعيد أحمد سودين البلوشي
باحث أكاديمي
أكاديمية الإمارات للهوية والجنسية

الملخص:

هدفت هذه الدراسة إلى تقييم استدامة الريادة الخدمية في مراكز سعادة المتعاملين من خلال دراسة تطبيقية أجريت في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ في دولة الإمارات العربية المتحدة. استخدم البحث المنهج الوصفي التحليلي، وذلك باستخدام الاستبيان كأداة أساسية لجمع البيانات. وتم تطبيق الاستبيان على عينة مكونة من 962 عاملاً في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن الموانئ.

وتشير نتائج الدراسة إلى وجود مستوى عالٍ من تطبيق القيادة الخدمية في مراكز سعادة المتعاملين من وجهة نظر موظفي الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ. وبلغ المتوسط الحسابي للبيانات المتعلقة بواقع القيادة الخدمية 120.4، بانحراف معياري قدره 332.1. علاوة على ذلك، تكشف الدراسة عن إنجاز كبير في استدامة القيادة الخدمية في مراكز سعادة المتعاملين من وجهة نظر نفس مجموعة الموظفين. وبلغ متوسط قيمة العبارات المتعلقة باستدامة القيادة الخدمية 579.3 بانحراف معياري قدره 062.1

وقد لوحظت فروق ذات دلالة إحصائية عند مستوى 50.0 في استجابات أفراد عينة الدراسة حول واقع القيادة الخدمية في مراكز سعادة المتعاملين حسب الجنس ولصالح فئة الإناث. بالإضافة إلى ذلك، لوحظت فروق ذات دلالة إحصائية حسب المسمى الوظيفي لصالح فئة مدير المركز.

ومع ذلك، لم توجد فروق ذات دلالة إحصائية عند مستوى 50.0 في استجابات أفراد عينة الدراسة حول واقع القيادة الخدمية في مراكز سعادة المتعاملين تبعاً لمتغيرات مثل العمر، والمؤهل العلمي، وعدد سنوات الخبرة

وكشف التحليل الإضافي عن وجود فروق ذات دلالة إحصائية عند مستوى 50.0 في استجابات عينة الدراسة حول مستوى استدامة القيادة الخدمية في مراكز سعادة المتعاملين تبعاً لمتغير المسمى الوظيفي. ومن الجدير بالذكر أن هذه الفروق لصالح فئة مديري المراكز، مما يشير إلى أن هذه الفئة هي الأكثر وعياً بمستوى استدامة القيادة الخدمية في مراكز سعادة المتعاملين

الفصل الأول: الإطار العام للدراسة

- **مقدمة:**

في ظل التطورات الاقتصادية والتكنولوجية المستمرة والمتزايدة في عالم الأعمال والخدمات، اتجهت العديد من الهيئات والمؤسسات الخدمية الى البحث عن مفاهيم جديدة ومتميزة، تسهم في إتاحة الفرصة أمامها للنمو والازدهار، لذا اتجهت العديد من تلك الهيئات والمؤسسات الخدمية الى بلورة فكرة ريادة الخدمات كوسيلة مهمة لتطويرها ورفع مستوى أدائها، وخاصة بعد أن أصبحت الريادة من سمات التطوير لتلك الهيئات والمؤسسات على المستوى العالمي

فقد اكتسب مصطلح الريادة بشكل عام وريادة الخدمات خاصة أهمية خاصة في العقود الأخيرة يمكن وصفها بالمتصاعدة على خلفية التقدم التكنولوجي والثورة الرقمية، ورغم أن الريادة pihsruenerpretnE، ليست بالمصطلح الجديد، إذ استخدمت لأول مرة في القرن التاسع عشر من قبل ريتشارد كانتيون وجان باتيست ساي، إلا أن أنها قد تم تسليط الضوء عليها بكثافة مؤخرا، نظرا للدور التنموي الذي لعبته خاصة في الاقتصادات الصاعدة. إذ تسهم ريادة الخدمات في زيادة دخل صاحب المشروع ودخل المجتمع مما يساعد في الحفاظ على النمو الاقتصادي والتنمية، كما تعد واحدة من اهم المصادر التي تساهم في الحفاظ على المجتمع والبيئة، بما تقدمه من فرص جديدة للعمل وإنشاء مشاريع صديقة للبيئة مما يحقق التنمية المستدامة (خطاب ومحمد، 0202)

وتبعا لذلك فقد أولت كافة الدول ومنها دولة الإمارات ملف رياده الخدمات اهتماما كبيرا نظرا لما ينعكس على تحقيقها للتنمية المستدامة، حيث أصبحت رياده الخدمات مجالا قويا ومعبرا نحو تحقيق التنمية المستدامة، وهذا بالتأكيد راجع لقدرتها على أحداث تأثيرا إيجابيا داخل مجتمع الأعمال والخدمات العالمية، هذا بالإضافة لما تقدمه من أطار جديد للابتكار والتنمية، وقدرتها على أن تقدم حلولا واقعيه تتماشى مع كافه المشكلات والتحديات الاقتصادية في كافة قطاعات الاقتصاد (غازي، الجزار، 0202)

ونظرا لأهمية الاستدامة، وزيادة وعي المجتمع الإماراتي بأهميتها فقد سعت جميع المؤسسات والمنظمات وخاصة المؤسسات الخدمية الى تطبيق مبادئها، من خلال الموازنة بين المتطلبات الاقتصادية، البيئية، الاجتماعية، والنظم والعمليات الداخلية بما يخدم الأجيال القادمة. فاستدامة ريادة الخدمات تسعى للكشف عن مدى تأثير المؤسسة الخدمية على البيئة الخارجية والمتضمنات الناتجة عن المستقبل، فالمنشأة الخدمية تعد جزء من نظام اجتماعي بيئي واقتصادي أكبر وتؤثر عملياتها على المجتمع والبيئة المحيطة،

ومن ثم اهتمت مقاييس الاستدامة بمعدل استهلاك المنظمة للموارد الاقتصادية والبيئة، مما يتطلب الحاجة الى زيادة الكفاءة في استخدام الموارد (البارودي، 7102).

ولهذا جاءت هذه الدراسة للكشف عن مدى استدامة الريادة الخدمات في مراكز إسعاد المتعاملين من خلال دراسة تطبيقية على الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ

- **مشكلة الدراسة:**

منذ أن أطلقت الأمم المتحدة مفهوم التنمية المستدامة، تسابقت الدول نحو تطبيق هذا المفهوم، وفقا لما يتوافق مع طبيعة وهيكل اقتصاداتها، وعلى الرغم من أن محاور التنمية المستدامة واحده وفقا لما وضعته الأمم المتحدة إذ عرفتها بأنها «التنمية التي تلبي احتياجات الجيل الحالية دون المساس بقدرة الأجيال المقبلة على تلبية احتياجاتها مستقبلا»، ألا أنها تختلف في أليه التطبيق وفقا لرؤيه وإستراتيجيه كل دوله ووضعها الاقتصادي (غازي، الجزار، 2020).

وعلى صعيد أخر تعد ريادة الخدمات من المواضيع المهمة التي حازت في مؤخراً على اهتمام أصحاب المنظمات على اختلاف أنواعها وأنشطتها، إذ أصبحت هذه المنظمات تهدف الى تحقيق التفوق واكتساب المزايا التنافسية من خلال تبني بعض المداخل التطويرية، وبرزت الريادة كأحد المداخل التي لقت اهتماماً كبيراً في المنظمات التي تتطلع الى تحقيق التنمية المستدامة، بل اعتبرها خياراً استراتيجياً لا يمكن التخلي عنه خاصة في ظل التطورات المتسارعة التي يعيشها العالم. ومما سبق يمكن تحديد مشكلة الدراسة من خلال السؤال الرئيس التالي

ما مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ؟

- **أسئلة الدراسة:**

سعت الدراسة للإجابة عن الأسئلة التالية:

1. ما واقع ريادة الخدمات في مراكز سعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ؟
2. ما مستوى استدامة ريادة الخدمات في مراكز سعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ؟
3. هل توجد فروق دالة احصائيا بين استجابات عينة الدراسة حول واقع ريادة الخدمات في

مراكز سعاد المتعاملين تعزى لمتغير (النوع – الخبرة –العمر- الوظيفة- المؤهل الدراسي)؟

4. هل توجد فروق دالة احصائيا بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغير (النوع – الخبرة –العمر- الوظيفة- المؤهل الدراسي)؟

- **أهداف الدراسة:**

هدفت الدراسة الى تحقيق الأهداف التالية:

1. التعرف على واقع ريادة الخدمات في مراكز سعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ.
2. الكشف عن مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ.
3. تحديد الفرق بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغير (النوع – الخبرة –العمر- الوظيفة- المؤهل الدراسي).
4. تسليط الضوء على الفرق بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغير (النوع – الخبرة –العمر- الوظيفة- المؤهل الدراسي).

- **أهمية الدراسة:**

تلفت انتباه واهتمام العاملين في قطاع الخدمات لأهمية تبني ريادة الخدمات، وتساهم في فهم متطلبات أو مقومات استدامة ريادة الخدمات في مراكز إسعاد المتعاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ؛ وتدعم جهود الهيئة في الحفاظ على ريادة خدماتها. كما يمكن أن تستفيد الجهات الحكومية الأخرى من نتائج هذه الدراسة في تطوير وتحسين خدماتها؛ حيث يؤمل ان تفيد نتائج هذا الدراسات المسؤولين في رسم سياسات تساعد في تحقيق التنمية المستدامة في مجال الخدمات. ومن ثم فإن هذه الدراسة أيضاً تثري المكتبات العربية بمرجع حديث في مجال استدامة الخدمات.

- **حدود الدراسة:**

الحدود الموضوعية: ستقتصر حدود الدراسة الموضوعية على ريادة الخدمات والاستدامة.

الحدود الزمانية: خلال عام 4202م.

الحدود المكانية: ستقتصر الحدود المكانية الإمارات.

الفصل الثاني الإطار النظري:

المحور الاول: الاستدامة

- **مفهوم الاستدامة:**

أصبح مفهوم الاستدامة أحد أهم الحقول الإدارية التي لاقت اهتماماً في الآونة الأخيرة وخصوصا في المنظمات التي تفكر بالبقاء طويل الأجل. لكون أهم معطيات الاستدامة هو الاعتماد على الخصائص الداخلية والخارجية للمنظمة وان تتوافق وتتوائم هذه الخصائص سوية لأجل محافظة المنظمة على تماسكها في الأجلين المتوسط والطويل، وأصبحت الاستدامة مفهوم أساسي للعديد من الباحثين والممارسين في مجال إدارة الأعمال وذلك ضمانا لسلامة وبقاء المنظمة، لذا تناول عديد من الباحثين تعريف الاستدامة، ومنهم:

عرفها أبو النصر ومحمد (7102) بأنها «تنمية حقيقية مستمرة متواصلة هدفها وغايتها الإنسان، تؤكد على التوازن بين البيئة بأبعادها الاقتصادية والاجتماعية والسياسية، بما يسهم في تنمية الموارد الطبيعية، وتمكين وتنمية الموارد البشرية، وإحداث تحولات في القاعدة الصناعية والتنمية على أساس علمي مخطط، وفق استراتيجية محددة لتلبية احتياجات الحاضر والمستقبل على أساس من المشاركة المجتمعية، مع الإبقاء على الخصوصية الحضارية للمجتمعات.» (ص13)

وعرفها بن بشير(2202) بأنها» برامج عمل مغيرة من استكشاف للموارد، وطريقة استغلالها والآلات المستعملة إلى المؤسسات التي تعمل على القيام بهذه المهمات، بناءً على الحاضر والمستقبل بمعنى أنها ليست قوالب جاهز طبق بل مُغيرة طبقًا للمعطيات المتوفرة والمتعلقة بالموارد والآلات أي التقنية المتوفرة والمؤسسات التي شرف على ذلك، وهو ما ينص عليه «مؤتمر بور نتلاند» ليس التنمية المستدامة وضع متزن وإنما هي مسار تغير أو هي مسار مُغير يؤخذ فيه بعين الاعتبار الموارد الموفرة، والاستثمار، والتطور التقني، والمؤسسات في علاقة بالحاضر والمستقبل»(ص87).

وعرفها والي(3202) بأنها «التنمية الحقيقية ذات القدرة على الاستقرار والاستمرار والتواصل من منظور استخدامها للموارد الطبيعية ، والتي يمكن أن تحدث من خلال استراتيجية تتخذ التوازن البيئي كمحور ضابط لها، ذلك التوازن الذي يمكن أن يتحقق من خلال الاطار الاجتماعي البيئي، والذي يهدف الى رفع مستوى معيشة الافراد من خلال النظم السياسية والاقتصادية والاجتماعية والثقافية التي تحافظ على تكامل الاطار البيئي، من خلال استخدام الاساليب العلمية والعملية والتي تنظم استخدام الموارد البيئية وتعمل

على تنميتها في نفس الوقت، وهي التنمية التي تستجيب لحاجات الحاضر دون المساومة بقدرة الاجيال المستقبلية على تلبية احتياجاتها الخاصة» (ص1).

- **اهمية الاستدامة:**

تعتبر التنمية المستدامة حلقة الوصل بين الأجيال، والضامن لاستمرار الحياة البشرية، وتضمن للأجيال القادمة التوزيع العادل للموارد، والعيش الكريم في الدولة الواحدة، وبين الدول المتعددة. وترجع أهميتها كونها الوسيلة المهمة لتقليص الفجوة بين جميع الدول المتقدمة والنامية، كما أنها تلعب دوراً في تقليص التبعية الاقتصادية للخارج، وتحسين مستوى المعيشة، ورفع مستوى التعليم، وتوزيع الإنتاج، وحماية البيئة، والعدالة الاجتماعية، وتوفير رؤوس الأموال، ورفع مستوى الدخل القومي. ولكي يتم تقليص هذه الفجوة وتحقيق كل هذه الأولويات لابد أن يكون لدينا رؤية استراتيجية محددة ومدروسة؛ لنتمكن من ترك إرث للجيل القادم. كما أنها تمثل حلقة وصل بين العالم شماله وجنوبه وتكامل للمصالح بينهما، وسداد لدين الدول المتقدمة التي استنزفت موارد الدول لنامية أثناء الاستعمار (أبو النصر، ومحمد، 7102).

- **أهداف الاستدامة**

1. تحقيق نوعية حياة أفضل للسكان، واحترام البيئة الطبيعية، وتعزيز الوعي لدى السكان بالمشكلات البيئية القائمة من أجل استخدام الموارد واستغلالها بشكل عقلاني، والعمل على ربط التكنولوجيا بالأهداف العامة للمجتمع، والعمل على إحداث تغير مستمر في احتياجات المجتمع وأولوياته.
2. تنمية مهارات الموارد البشرية وقدراتهم، حيث إن العنصر البشري هو العنصر الأهم في تحقيق التنمية المستدامة وبالتالي فمن الضروري العمل على تنمية القوى البشرية والاعتناء بها من مختلف النواحي.
3. الحفاظ على مصالح الأجيال المستقبلية من خلال ترشيد استهلاك الموارد الحالية المتاحة، والعمل على الحد من تراكم الديون، والتي قد ينتج عنها حالة تنموية هشة بالإضافة إلى الحد من إمكانية التعرض لمشكلات بيئية ناتجة عن الإفراط في استخدام الموارد البيئية المتاحة.
4. توفير فرص العمل إذ يمكن أن تحفز السياسات الاقتصادية الكلية وكذلك سياسات التنمية ونهضة مبادرات اقتصادية جديدة ترتبط مع التنمية المستدامة من خلال الحوافز التي تحفز أنماط أكثر استدامة من الاستهلاك والإنتاج على الصعيد الدولي

ويمكن أن يسهم تشجيع القطاعات الجديدة غير الملوثة ولا سيما الخدمات وتحويل توجه الأنشطة الاقتصادية باتجاه توفير فرص الوظائف في القطاعات المستدامة بيئيًا (فتيحة، 2017).

- **خصائص الاستدامة:**

لقد حددت دراسة خصائص التنمية المستدامة في التالي (أبو النصر ومحمد،7102) :

تستند على فكرة العدالة بين الأفراد والأجيال، بالإضافة إلى التركيز على دور المجتمع المدني ومنظماته ودور جميع شرائح المجتمع في تطوير الأنشطة للمساهمة في تحسين المستوى المعيشي لأفراد المجتمع المدني

تهدف إلى الحد من زيادة الفقر في العالم من خلال تحقيق التوازن بين النظم البيئية والاقتصادية والاجتماعية وتحقيق الرفاهية الاجتماعية.

تتميز بمزيد من التداخل والتعقيد من التنمية عامة، خاصة من حيث الطبيعة والمجتمع، بالإضافة إلى وجود أبعاد روحية وثقافية تتعلق بالحفاظ على خصوصية الحضارة الاجتماعية.

تعتبر تطورًا طويل الأمد ويعتمد على تقييم الإمكانات الحالية، مع مراعاة حقوق الأجيال القادمة في الموارد الاجتماعية المتاحة

عناصرها مترابطة، ولا يمكن قياس مؤشراتها بسبب تداخل أبعادها الكمية والنوعية.
تركز على جميع الموارد المتوفرة في الدولة، ورفع الوعي بالحفظ والاستثمار، لأن استمرار التنمية مرهون بقرارات الإنسان، لذلك فإن تمكين الإنسان وتعليمه وتنظيمه هو وظيفتها الأولى.

كما حدد دراسة (5102,ylbmessA) خصائص التنمية المستدامة في الخصائص التالية:

تنمية تراعي الاجيال القادمة بالموارد ونظافة البيئة- بنفس القدر الذي تتمتع به الأجيال الحالية

تنمية طويلة الاجل، حيث تعتمد على نتائج الخطط التنموية والسياسات الاقتصادية على المدى القريب، ثم تستمر على المدى البعيد.

تنمية تسعى الى تحقي العدالة بين الأفراد، وبالتالي توزيع الثروة بشكل عادل.
تعتمد بشكل كبير على التقنية التي توفر الوسائل والتجهيزات، بالإضافة الى الكوادر المؤهلة

تنمية تسعى الى الحفاظ على نظافة البيئة وحمايتها، ومحاربة كل أشكال التلوث.

تنمية تسعى للحفاظ على الموارد الطبيعية الى أقصى حد ممكن من خلال ترشيد استهلاكًا، أو إيجاد بدائل ملائمة.
تنمية تقوم على التنسيق بين جميع شرائح المجتمع.

- **مبادئ الاستدامة:**

فيما يتعلق بالمبادئ الأساسية للاستدامة فهي تدور بشكل رئيس حول المقومات السياسية

والاجتماعية والأخلاقية وأهم هذه المبادئ كما حددتها دراسة الخطيب، (3202)، صخراوي (1202) على النحو الآتي:

الإنصاف: عن طريق حصول كل فرد على حصة عادلة ومتوازنة من ثروات المجتمع، حيث يشكل مبدأ الإنصاف شرطًا جوهريا لتحقيق التنمية المستدامة لكافة الشعوب، بل ويعتبر تجسيده أساسًا لمصداقية جميع السياسات الرامية إلى تحقيق أهداف التنمية المستدامة على المستوى الدولي والوطني، وقد ركز المتفاوضون في مؤتمر ريو لعام 2991م في جوانب عديدة من جدول الأعمال على مبدأ الإنصاف بشكل عام، والإنصاف داخل الجيل الواحد بشكل خاص.

التمكين: إعطاء كل فرد في المجتمع فرصة المشاركة الكاملة الفعالة في صنع القرارات أو التأثير، فوفقا لأحكام القانون الدولي للبيئة، يجب أن يحرص كل جيل على مراعاة الحقوق البيئية للجيل الذي يليه، واستخدام الموارد الطبيعية على نحو مستدام وصيانة عناصر البيئة الطبيعية وحمايتها، والعمل على تنويع الخيارات التنموية، وتوزيع ثمارها على نحو منصف داخل كل جيل، إلا أن هذا المبدأ الذي يقع في صميم التنمية المستدامة، لا يمكن تجسيده في أرض الواقع بمعزل عن إدماج الاعتبارات البيئية في سياسات التنمية، ومراعاة متطلبات التنمية عند صياغة وتطبيق وتفسير الالتزامات البيئية وهو ما يجعل من الإدماج مبدأ أساسيًا من مبادئ التنمية المستدامة

التضامن بين الأجيال وبين فئات المجتمع المختلفة، بهدف الحفاظ على البيئة والموارد الطبيعية، يستمد هذا المبدأ مضمونه من اليقين التام بأن الانتماء إلى الجيل الحاضر لا يعني أبدا تجاهل حقيقة كون الأرض ميراثا للأجيال التي ستأتي في المستقبل، وهو ما يستشف من تعريف التنمية المستدامة الذي أورده تقرير برونتلاند لعام 7891م بأنها : «التنمية التي تفي باحتياجات الحاضر، دون الإخلال بقدرة الأجيال المقبلة على الوفاء باحتياجاتها ، وأكده المبدأ 3 من إعلان ريو لعام 2991م الذي اعتبر حق التنمية وسيلة منصفة لتلبية الاحتياجات التنموية والبيئية للأجيال المقبلة

حسن الإدارة والمساءلة: من خلال خضوع أهل الحكم والإدارة إلى مبادئ الشفافية والمراقبة، سواء كان ذلك على مستوى المجتمع الدولي، من حيث مشاركة الدول وتمثيلها في المنظمات البيئية، أو على المستوى الوطني من حيث مشاركة الجمهور في مسار اتخاذ القرارات التنموية التي من شأنها أن تؤثر بشكل سلبي في بيئة وصحة السكان ونوعية حياتهم على المستوى المحلي.

المحور الثاني: مفهوم ريادة الخدمات

- **مفهوم الريادة:**

يعد مفهوم الريادة مفهوماً قديماً، واستعمل لأول مرة في اللغة الفرنسية في بداية القرن السادس عشر، وقد تضمن المفهوم آنذاك معنى المخاطرة وتحمل الصعاب التي رافقت حملات الاستكشاف العسكرية، ودخل مفهوم الريادة إلى النشاطات الاقتصادية في مطلع القرن الثامن عشر من قبل nollitnaC drahciR الذي وصف التاجر الذي يشتري سلعاً بسعر محدد، لبيعها في المستقبل بسعر لا يعرفه مسبقاً بأنه ريادي. ولا تقصر الريادة على التطوير والتحديث واستخدام الأفكار المبدعة في تقديم منتج أو خدمة متميزة غير مسبوقة باستخدام مبادئ اقتصادية بحتة كترشيد استهلاك الموارد وزيادة الإنتاج، ولكن تمتد لتشكل تحقيق الكفاءة الاقتصادية، لذلك فهي تتضمن إنشاء مشروع عمل جديد يقدم قيمة اقتصادية مضافة من خلال إدارة الموارد بكفاءة وأهلية متميزة لتقديم شيء جديد أو ابتكار نشاط اقتصادي وإداري جديد (مرهج،0202).

اختلف الباحثون في تعريفهم لمفهوم الريادة وتحديد أبعادها، فقد عرفها (namhcaR, late 1102 ,931P) بأنها إنشاء شيء جديد ذي قيمة وتخصيص الوقت والجهد والمال اللازم للمشروع، وتحمل المخاطر المصاحبة واستقبال المكافأة الناتجة بما يحقق تراكم الثروة

ويرى لطفي (9102) إن التوجه الريادي لا يمكن فهمه بشكل كاف بدون تحليل كل من سلوك الفرد والبيئة المحيطة بشكل تكاملي، ويمكن وضع خصائص سلوك الفرد السمات التالية:

1. السمات الشخصية كميلهم للتحدي، واحتياجهم لإنجاز، قدرتهم على ضبط النفس والقدرة نموذج القدوة أو المثل الأعلى في البيت أو في العمل.
2. الديموغرافيا: مستويات العمر والتعليم والوضع الاجتماعي والاقتصادي والخبرات.
3. السلوك اتجاه النفس مستويات الثقة بالنفس والسلوك والاهتمامات الشخصية وميل

الأفراد لتوهم قدرتهم على السيطرة على المواقف.

4. الواقع السياسي والقانوني والاقتصادي والثقافي للمجتمع المحيط.
5. العلاقات الإنسانية ومستوى الثقة وتأثيرهم في الاقتصاد فكلما زادت الثقة والعلاقات الإنسانية قل القلق والزيف على التعامل مع المجهول.

- **مفهوم ريادة الخدمات:**

تعريفها دراسة ((azeR ,te .la ,6102بأنها «التعرف على الفرص واغتنامها وتحويلها إلى سلع وخدمات قابلة للتسويق، وإضافة قيمة لها من خلال استغلال الوقت والموارد وتحمل المخاطر وتحقيق الربح، وباختصار فإن إيجاد أو إضافة قيمة جديدة من الخصائص المميزة لريادة الخدمات» (99).

- **أهمية ريادة الخدمات**

إن تحقيق الريادة يعني بلوغ المنظمات لذاتها ومن ثم متابعة المستجدات ذات العلاقة وهذا يفترض عليها توظيف إسهاماتها بغية الكشف عن أهميتها ومن ثم التحري عن مردوداتها في أطار دورها المتمثل في إحداث أثار إيجابية تتمثل بالآتي:

1. إحداث التغيير والتحول إذ يعد الإبداع من الصفات المميزة للريادية خاصة وان المنظمات الريادية تعمل كدالة للتغيير من خلال ممارسات النشاطات الريادية.
2. إيجاد العديد من المشروعات التي تعد مهمة لتطوير الاقتصاد وتنميته.
3. إيجاد فرص العمل المهمة على المدى الطويل من اجل تحقيق النمو الاقتصادي.
4. زيادة الكفاءة بزيادة التنافسية، أي ان دخول منافسين جدد يحفز المنظمة للاستجابة بشكل كفوء وفعال.
5. إحداث التغيير في هيكل السوق والعمل من خلال زيادة تبني الابتكار التنظيمي والتقنيات الحديثة.
6. احتمالية إدخال ابتكارات جذرية يترك أثرا إيجابيا في الاقتصاد بشكل كامل نتيجة البداء بأنشاء المنظمات الجديدة.
7. التنوع النوعي والكمي الكبير، إذ إن المشاريع الجديدة تقدم أفكارا جديدة، إبداعيا واقتصاديا (نعمة، الورد، 0202)

- **أبعاد ريادة الخدمات:**

تتكون ريادة الخدمات يتكون من ثلاثة أبعاد رئيسية يمكن أن تستخدم لقياس التوجه

الريادي لخدمات وهذه الأبعاد هي:

1. **الإجراءات الاستباقية:** هي اتخاذ الإجراءات والمبادرة من خلال اكتشاف الفرص المتاحة، والبحث عن الأسواق التي تدعم من المركز التنافسي للمؤسسة، وقدرتها وجاهزيتها على تقديم المنتجات الجديدة التي تتميز بهما عن المؤسسات الأخرى في ذات الصناعة، فالإجراءات الاستباقية تشير قدرة المؤسسة على مواجهة الظروف المحتملة، والتفوق على المنافسين من خلال تهيئة العاملون فيها، واستخدام الموارد بطريقة كفؤة، ودراسة السوق وعوامله، مما يتيح لها القدرة على التنبؤ بتحركات المنافسين، والتحرك على أساسها، وهذا يتطلب منها أن تعمد إلى التخطيط الاستراتيجي، لمعرفة الأداء التشغيلي والأداء التنافسي والأداء المالي لها
2. **الإبداع:** هو العملية تتطلب التعاون والتنسيق بين الوحدات الإدارية داخل الشركة تهدف إلى تبني الأفكار الجديدة سواء التي تتعلق بإنتاج سلعة أو تقديم خدمة جديدة ووضعها موضع التنفيذ من أجل تحقيق أهداف المنظمة وزيادة قدرتها على مواجهة المنافسة من المنظمات الأخرى وتلبية حاجات ورغبات وتوقعات عملائها داخل السوق المستهدف (أحمد، 9102).
3. **استغلال الفرص:** تمثل عملية استغلال الفرص أحد أساسيات الريادة في منظمات الأعمال والتي تعني كيفية خلق أو اكتشاف الفرصة في البيئة المحيطة وتطويرها وتوفير الإمكانيات والموارد اللازمة لاستغلالها والاستفادة منها في اشباع الحاجات والرغبات غير المشبعة لدى العملاء واستخدامها في مواجهة المنافسة داخل السوق.
4. **تحمل المخاطر:** وتعني قدرة منظمات الأعمال على تحمل المخاطر الناتجة عن الأعمال الريادية، وهذه المخاطر تتمثل في مخاطر الرغبة في تبني الأفكار الجديدة المبتكرة ومخاطر توفير الموارد الأساسية اللازمة لاغتنام الفرص المتاحة أمام الشخص الريادي الذي يتحمل مسؤولية فشل هذه الأفكار أو الفرص (أبو حمادة، ونصار، 6102).

- **كفايات ريادة الخدمات**

يربط الاقتصاديون غالباً الخدمات الريادية بالإبداع والمخاطرة والقدرة على حسن استغلالها الحديثة وتطبيقها، وتنوعت الكفايات والمهارات التي تندرج تحت ريادة الخدمات، والتي يجب أن يمتلكها الريادي للنجاح في عمله، ويمكن تحديد هذه الكفايات والمهارات فيما يلي:

1. القدرة على تحمل المسئولية.

2. المبادرة التي تتخطى متطلبات العمل.
3. الانتباه إلى الفرص واقتناصها. الإصرار، والمثابرة، والالتزام بالعمل والمتابعة. البحث عن المعلومات اللازمة للعمل.
4. الاهتمام بالجودة والنوعية. الفاعلية والتخطيط المنظم. القدرة على حل المشكلات.

- **مداخل دراسة ريادة الخدمات:**

المدخل الاقتصادي: ظهر الاهتمام بالمقاولات في الاقتصاد الحديث في نظرية التنمية الاقتصادية التي طرحت سنة (1191) التي أكدت على أن رواد الأعمال هم جوهر التنمية الاقتصادية، فهم الذين يخلقون التغييرات ضمن الاقتصاد من خلال تقديم المنتجات والخدمات الجديدة، وطرائق الإنتاج الجديدة، والأشكال التنظيمية الجديدة، وفتح الأسواق الجديدة، واستعمال مصادر تجهيز جديدة

المدخل (النفسي – الاجتماعي): ترجع جذور ظهور هذا المدخل عندما ناقش (dnallelccM، snilloC) أهمية العوامل النفسية -الاجتماعية للأفراد كمسببات للأعمال الريادية وهناك عوامل اجتماعية وخصائص يتأثر بها المحيط الاجتماعي والمعايير الاجتماعية والقيم والثقافة التي تدعم أو تعيق الأعمال الريادية أو السلوك المقاولاتي

مدخل السلوك الريادي تقوم المنظمات على وفق هذا المدخل بتطوير وتحسين منتجاتها وخدماتها استجابة للتغيرات والمستجدات البيئية والتنافسية.

مدخل المنظمة المتعلمة ويمكن أن يسمى بمدخل التوجه نحو التغيير، اذ يتطلب الرؤيا الريادية) في سعي المنظمة لتحقيق الأداء المتوقع ومساعدة العاملين على المشاركة في كيفية وضع الطرائق الملائمة للمنافسة.

مدخل القيادة الإستراتيجية يؤدي القادة على وفق هذا المدخل ادواراً فاعلة ومؤثرة لضمان امتلاك المنظمة رؤيا واضحة ومفهومة وموجهة ومدعومة بهيكل تنظيمي ملائم وثقافة إدارية ونظام مكافآت الضمان تحفيز المستخدمين والتزامهم.

مدخل التوجه الريادي بالاستفادة من القدرات والموارد على وفق هذا النموذج تحدد المنظمة أولا أين تريد أن يكون مستواها من الكثافة الريادية، وتحدد هل أن الجهود الريادية للمنظمة ستكون موجهة نحو خدمات جديدة أو نحو أسواق جديدة، ومن ثم تحدد الموقع الذي تريد أن تكون فيه القائدة للإبداع مقابل التابعة للإبداع (أحمد، 9102)

المعوقات التي تواجه ريادة الخدمات:

تواجه ريادة الخدمات العديد من المعوقات يمكن ايجازها في التالي: -

القيم الاجتماعية السائدة، التي لها دور في تكوين البناء الاقتصادي وكذلك الاجتماعي والثقافي والسياسي للمجتمعات، فهي الإطار المرجعي للسلوك الفردي وهي الدافعة للسلوك الجمعي وتحتاج ثقافة ريادة الأعمال إلى أنماط سلوكية جديدة وبالتالي تحتاج إلى قيم جديدة تدفعها إلى الطريق الصحيح

صعوبة إحداث تغيير في بعض أنماط الشخصية مثل الانعزالية والتواكل وعدم احترام قيم العمل خاصة اليدوي أو عدم الإيمان بالجديد والخوف من المستحدثات وعدم الاعتراف بأهمية المرأة ودورها في المجتمع مما ينتج عنه تعطيل طاقات نصف المجتمع بجانب عدم احترام وتقدير قيمة الوقت.

وجود موروثات ثقافية في بعض الأمثال الشعبية تحض الأفراد على التمسك بالوظائف الحكومية باعتبارها أكثر أماناً، والتمسك بالتبعية وعدم التجديد والابتعاد عن المخاطرة.

معوقات إدارية وقانونية، وتظهر في تعقد الإجراءات والاستغراق في الروتين والبطيء الشديد في إصدار القرارات وانتشار اللامبالاة والسلبية وسيطرة العوامل الشخصية على علاقات العمل الرسمية والقصور في الكفاءات الإدارية

الخوف من الجديد، حيث يخشى كثير من الأفراد في أحيان كثيرة أن يتحملوا عبء تجربة جديدة لا يعرفون نتائجها وتسهم خبراتهم السابقة في تشجيعهم على الإقدام على قبول التجربة أو المشاريع الجديدة

عدم توافر النوعية من القيادات القادرة على تحريك الأفراد والجماعات وإثارتهم نحو تحقيق هدف مشترك جديد وحثهم نحو استخدام الموارد المتاحة بصورة أفضل لتحسين مستواهم

عدم توافر الموارد التكنولوجية التي يمكن استخدامها لإحداث تغيير في قيم المادة والسلوك من حالة حاضرة إلى حالة مستقبلية

نقص الوعي بالمشاركة بين الأفراد وعدم توافر الرغبة والاقتناع بأهميتها منذ الطفولة وفي المراحل الدراسية الأولى إلى أن يخرج الإنسان لمزاولة العمل الخاص به (العتيبي، 5102)

ريادة الخدمات والتنمية المستدامة:

تقوم التنمية المستدامة على تطوير المدن والمجتمعات بالإضافة إلى الأعمال التجارية مما يتطلب استخدام الموارد الطبيعية لتحسين الظروف المعيشية للأفراد بطريقة لا تحتمل الإسراف أو الإيذاء كما في حال التلوث البيئي مثلا أو ما يحصل من ندرة المياه الصالحة للشرب كما أن التنمية المستدامة تشمل مجالات كثيرة مثل النمو الاقتصادي والتنمية الاجتماعية بالإضافة الى الحفاظ على البيئة والموارد الطبيعية وهنا يكمن دور

ريادة الأعمال في ابتكار طرق جديدة وليست الطرق المعتادة التي تسبب الاستنزاف والتلوث وذلك من أجل استثمار الطاقات البشرية وموارد الطبيعة بحيث تنعكس نتائجها إيجابا على كل من الأفراد حاليا ومستقبليا مثل الابتكار من أجل استثمار وسائل الطاقة البديلة كابتكار سيارات الكهرباء التي تحد من التلوث الهوائي وغيرها الكثير من الأمثلة وبالتالي فإن ريادة الإعمال هي أداة أساسية للتنمية المستدامة وتطوير ريادة الأعمال له دور كبير في تحقيق وتفعيل التنمية المستدامة خصوصا إذا تم توجيهها نحو ذلك (غازي والجزار، 0202)

أبعاد استدامة الخدمات.

تضم استدامة الخدمات عدة ابعاد متكاملة ومتداخلة ينظر اليها بشكل تكاملي، ويمكن توضيح

مفهوم الاستدامة والتعامل معها من خلال الأبعاد التالية:

1. **الاستدامة الاقتصادية:** تعرف استدامة الخدمات الاقتصادية بانها تأثير الشركات على الظروف الاقتصادية لأصحاب المصلحة وعلى النظام الاقتصادي الوطني والعالمي، والتي تنعكس على المجتمع وتدفق الموارد بين جميع أصحاب المصلحة، وتتمثل متطلبات الاستدامة الاقتصادية إدارة الشركة لعدة أنواع من راس المال الاقتصادي ومنها: راس المال المالي الدين وحق الملكية، وراس المال الثابت (الأراضي والآلات)، وراس المال غير الملموس (الشهرة وبراءة اختراع. ومن اجل تحقيق الاستدامة الاقتصادية، يجب على الشركة ممارسة الأنشطة بطريقة معترف بها مع تحقيق المنافع الاقتصادية والاجتماعية للمهتمين بها (نخلة ومسعد، 2202).
2. **الاستدامة الاجتماعية:** تعبر الاستدامة الاجتماعية عن الوعي بمسؤولية الشركة عما تقوم به من أفعال، والتزام الشركة الحقيقي على المدى الطويل بكافة الأنشطة التجارية من اجل بقائها في الأسواق بنجاح ولفترة زمنية طويلة، كما تهدف الاستدامة الاجتماعية إلى التأثير الإيجابي على كافة العلاقات الحالية والمستقبلية مع أصحاب المصلحة بتركيزها على تلبية احتياجاتهم من اجل تعزيز الولاء للمنظمة ، وتشمل الاستدامة الاجتماعية مفاهيم المساواة التمكين إمكانية الوصول والمشاركة وتقوية الهوية والاستقرار التنظيمي، كما تشتمل مسائل تتعلق بالتنمية البشرية كالتعليم والتدريب والصحة والسلامة المهنية في مكان العمل وتنمية القدرات والمساواة في كل من الرواتب والمنافع وتكافؤ الفرص وغياب التميز في مكان العمل والاعتبارات الأخلاقية مثل حقوق الموظفين والثقافة والقيم والعدالة بين الجميع

(2202 ,.la te irahsfA) .

3. **الاستدامة البيئية:** تتطلب الاستدامة البيئية المحافظة على رأس المال الطبيعي كمصدر للمدخلات الاقتصادية، وتشتمل أيضا على الإثار البيئية التي تنتج عن نشاط الشركة كأثار استخدام الموارد والغازات التي تنبعث في الهواء وفي الماء أو في الأرض وأيضا النفايات الخطرة وأيضا آثار التنوع البيولوجي والقضايا البيئية على مدى دورة حياة المنتج، تشير الاستدامة البيئية إلى الحفاظ على كافة الممارسات بحيث تشتمل الاستدامة البيئية النظم الإيكولوجية والقدرة على التنوع البيولوجي (2202.la te hamuJ)

الدراسات السابقة:

دراسة الطائي، أحمد هادي طالب. (6102). دور تبني الاستراتيجيات الريادية وتأثيرها في تحقيق الميزة التنافسية المستدامة: دراسة استطلاعية على شركة بغداد للمشروبات الغازية المساهمة المختلطة.

هدفت الدراسة إلى التحقق من تأثير تبني الاستراتيجيات الريادية المتمثلة بـ (الإبداع، الابتكار، أخذ المخاطرة، المبادأة) ودورها في تحقيق الميزة التنافسية المستدامة المتمثلة بـ (المقدرة الجوهرية، الجودة، الموضع التنافسي، تكنولوجيا المعلومات، المرونة الاستراتيجية) في عينة من المديرين في شركة بغداد للمشروبات الغازية المساهمة المختلطة حيث تم توزيع (84) استبانة على عينة قصدية من الإدارة العليا والوسطى وتمت الاستجابة بشكل كامل أي بنسبة استجابة 001 %. خلصت الدراسة إلى وجود علاقة تأثير وارتباط ذو دلالة إحصائية ما بين الاستراتيجيات الريادية والميزة التنافسية المستدامة وكان من أبرز النتائج وجود علاقة تأثيرية ذات دلالة إحصائية لكل من الاستراتيجيات الريادية على الميزة التنافسية المستدامة وبالتسلسل حسب الأقوى تأثيرا (الابتكار، أخذ المخاطرة، الإبداع، المبادأة) وخرجت الدراسة بتوصيات كان من أبرزها التأكيد على الجودة في المنتوج كونها كانت البعد الأكثر مستوى ممارسة من بين أبعاد الميزة التنافسية المستدامة. فضلا عن التركيز على التنويع في الإنتاج من حيث إدخال منتجات فريدة تتميز بها عن المنافسين مما يؤدي إلى استدامة التميز والريادة في السوق العراقية الأمر الذي يجعل الشركة المبحوثة في مقدمة الشركات العراقية تميزا.

دراسة بو حمادة، عبدالموجود عبدالله، و نصار، حمدي جابر محمد. (6102). ريادة الأعمال وجودة الخدمات الصحية داخل المستشفيات الحكومية بمنطقة تبوك.

هدفت الدراسة الى تحليل أثر التوجه نحو ريادة الأعمال في جودة الخدمات الصحية داخل المستشفيات الحكومية السعودية بمنطقة تبوك، من خلال جمع البيانات عن طريق قائمة استقصاء تم توجيهها إلى عينة حجمها 004 مفردة من المسئولين داخل هذه

المستشفيات والبالغ عددهم إحدى عشر مستشفى، مستخدماً المنهج الوصفي التحليلي. وقد توصلت الدراسة إلى مجموعة من النتائج أهمها ضعف توجه المستشفيات الحكومية السعودية بمنطقة تبوك نحو ريادة الأعمال، وأن بعد الإبداع احتل الترتيب الأول، ثم تحمل المخاطر، وأخيرا استغلال الفرص. وأن هناك اهتمام متوسط بجودة الخدمات الصحية داخل المستشفيات الحكومية السعودية بمنطقة تبوك، وأن بعد الملموسية احتل الرتيب الأول في درجة الاهتمام بينما بعد التعاطف احتل الترتيب الأخير. وأن كل بعد من أبعاد التوجه نحو ريادة الأعمال (الإبداع، تحمل المخاطر، استغلال الفرص) له أثر ذو دلاله إحصائية في الاهتمام بجودة الخدمات الصحية، وأن هذه الأبعاد مرتبة تنازلياً حسب درجة تأثيرها تتمثل في تحمل المخاطر، الإبداع وأخيراً استغلال الفرص

دراسة مرهج، منذر عبدالكريم، وحسن، باسم محمد. (0202). دور الريادة في تعزيز جودة الخدمة الفندقية: دراسة ميدانية على فنادق الأربع والخمس نجوم في مدينة اللاذقية.

هدفت الدراسة إلى تحديد دور الريادة في تعزيز جودة الخدمة الفندقية في فنادق الأربع والخمس نجوم في مدينة اللاذقية، وذلك من خلال دراسة العلاقة بين الريادة وأبعاد جودة الخدمة الفندقية (الملموسية، الاعتمادية، الاستجابة، التعاطف، الضمان) اعتمدت الدراسة على المنهج الوصفي التحليلي، وشمل عينة الدراسة فهي عينة عشوائية ميسرة بلغت (001) مدير، حيث تم توزيع الاستبانة أداة الدراسة عليهم، وتم استرجاع (19) استبانة صالحة وكاملة للتحليل الإحصائي، كما شمل مجتمع البحث جميع زبائن الفنادق ذات التصنيف الأربع والخمس نجوم في مدينة اللاذقية، حيث قام الباحث بالحصول على استجابات (19) زبون لمعرفة جودة الخدمة الفندقية المقدمة لهم من تلك الفنادق. توصلت الدراسة إلى مجموعة من النتائج أهمها: سعي الفنادق محل الدراسة للتوجه نحو الريادة في أعمالها، وبأهمية نسبية (32.77%)، وذلك من خلال الاستجابة لحالات التغيير ومواكبة المستجدات في بيئة الأعمال، وتنمية الأفكار الإبداعية وتحمل المخاطر واتخاذ المواقف الجريئة وتنمية الموارد على نحو إبداعي. كما أظهرت النتائج وجود علاقة طردية ودالة إحصائية بين توجه الفنادق محل الدراسة نحو الريادة في أعمالها وبين تعزيز جودة الخدمة الفندقية من خلال أبعادها

دراسة العمري، سامر فندي أحمد، ومقدادي، يونس عبدالعزيز. (0202). أثر استراتيجيات الريادة في تحقيق الاستدامة للمشاريع الصغيرة في مدينة إربد.

هدف الدراسة إلى قياس أثر استراتيجيات الريادة في تحقيق الاستدامة للمشاريع

الصغيرة في مدينة إربد، ولتحقيق أهداف الدراسة تم استخدام المنهج الوصفي التحليلي؛ حيث تم تطوير استبانة مكونة من (15) فقرة وتم التأكد من صدقها وثباتها، وقد تم توزيعها على عينة الدراسة وبنسبة 001% والذي بلغ عددهم الإجمالي (003) مشروعا. وأظهرت نتائج الدراسة وجود أثر ذو دلالة إحصائية لأبعاد الإبداع والابتكار الريادي والمخاطرة الريادية والتفرد الريادي على تحقيق الاستدامة (البقاء) بينما لا يوجد أثر ذو علاقة إحصائية في بعد المبادأة الريادة على تحقيق الاستدامة (البقاء)، وعدم وجود أثر ذو دلالة إحصائية للإبداع الريادي والابتكار الريادي والمخاطرة الريادية والمبادأة الريادية على تحقيق الاستدامة (النمو)، بينما يوجد أثر للتفرد الريادي على تحقيق الاستدامة (النمو)، وعدم وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد العينة على مقياس الاستراتيجيات تعزى لمتغير النوع الاجتماعي والعمر، ولكن أشارت الدراسة إلى وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد العينة على مقياس الاستراتيجيات تعزى لمتغير المؤهل العلمي والخبرة، وأوصت الدراسة عددا من التوصيات ومن أهمها ضرورة رفع كفاءة وقدرات مالكي المشاريع الصغيرة في محافظة إربد وذلك من خلال التحاقهم ببرامج تدريبية متخصصة بإدارة المشاريع الريادية واستراتيجياتها وذلك لتمكينهم من إدارة مشاريعهم بكفاءة وفعالية عالية لضمان البقاء والنمو واستدامتها، في ظل تحديات السوق التي تواجهها من حين لآخر

دراسة علي، رحاب علي إبراهيم، محمود، عبدالله عبدالرحيم إدريس، و حامد، عبدالسلام آدم. (0202). أثر التوجه الريادي على الأداء المستدام: دراسة على عينة من المؤسسات الخدمية بولاية الخرطوم.

هدفت الدراسة إلى معرفة أثر التوجه الريادي على الأداء المستدام في مؤسسات القطاع الخدمي بولاية الخرطوم، وقد استخدمت الدراسة المنهج الوصفي، استنادا إلى نظرية VBR ومراجعة الأدبيات، تم بناء نموذج الدراسة وفرضياتها اعتماداً على أدبيات الدراسة وكذلك تم الاستعانة بالدراسات السابقة في تطوير مقاييس الدراسة، وصممت استبانة لجمع البيانات من عينة غير احتمالية، حيث تم توزيع عدد (622) استبانة واسترد منها (612) بنسبة استجابة بلغت (85.59%)، وللتأكد من درجة الاعتمادية في البيانات تم استخدام اختبار الفا كرونباخ، واستخدم أسلوب تحليل المسار ونمذجة المعادلة البنائية لاختبار الفرضيات. وتم معالجة البيانات إحصائياً عن طريق (32V SOMA)، وقد توصلت الدراسة إلى مجموعة من النتائج منها: أن هنالك أثر جزئي للتوجه الريادي على الأداء المستدام، ووجود علاقة إيجابية ما بين التوجه الريادي ببعد (الإبداع والاستباقية) والأداء

المستدام، وعدم وجود علاقة بين التوجه الريادي ببعد (المخاطرة) والأداء المستدام بمؤسسات القطاع الخدمي بولاية الخرطوم، وبناء على هذه النتائج أوصت الدراسة بضرورة زيادة وعي المديرين بأهمية التوجه الريادي للمؤسسات الخدمية والذي بدوره يعزز أدائها ويقودها إلى الاستدامة

دراسة عياش، وجدان إبراهيم حنا، و الجوازنة، بهجت عيد. (1202). gnissessA dna llamS eht fo ytilibaniatsuS no tcapmI rieht dna srotcaF sseccuS eht .etaronrevoG qarfaM ni sesirpretnE lairuenerpertnE muideM

هدفت الدراسة إلى تقييم العوامل التي تؤثر على نجاح المشاريع الريادية الصغيرة والمتوسطة في محافظة المفرق والتي تعمل على استدامتها في الظروف الاقتصادية الصعبة التي يمر بها الأردن ككل والمفرق على وجه الخصوص. ولتحقيق أهداف هذه الدراسة استخدمت الدراسة التحليل الموضوعي في تفسير البيانات التي تم جمعها من إجراء 22 مقابلة مفتوحة مع أصحاب المؤسسات الريادية وممثلي المؤسسات الحكومية وغير الحكومية. لم تستطع الباحثة شمول جميع القطاعات في محافظة المفرق، لذلك ركزت على القطاع الزراعي في البادية الشمالية وقطاع الخدمات في مدينة المفرق ومنطقة رحاب وايدون. استخدمت الدراسة مزيجاً من المنهج الاستقرائي والاستنباطي لتشفير البيانات وتحليلها. ووجدت الدراسة مجموعة من العوامل التي تساهم في نجاح المشاريع الريادية في المفرق ، وأهمها: مدى توفر التمويل لإنشاء المشاريع والمحافظة على استمرارها و التوسع فيها ؛ تأهيل وتدريب العاملين في المؤسسات الصغيرة والمتوسطة؛ العوامل الفردية مثل سمعة الصدق وخدمة العملاء الجيدة والخبرة والرؤية والعمل الجاد والقدرة على إدارة المخاطر ؛ المهارات الإدارية والقدرة على توزيع المهام (تقسيم العمل) ؛ دراسة الجدوى واستخدام المحاسبة الإدارية؛ البحث والتطوير المستمر؛ الابتكار؛ إدارة المواد عن طريق رفع الجودة أو تقليل التكلفة أو كليهما ؛ الحفاظ على مكانة المنتج في السوق وإيجاد أسواق جديدة ؛ التعبئة والتغليف الجيد والتخطيط الجيد ضمن إطار زمني. قد تحتوي المشاريع الريادية على واحد أو كل هذه العوامل، تساهم هذه العوامل في إضافة قيمة إلى المشاريع الريادية الصغيرة والمتوسطة ومنحها ميزة تنافسية، تتبع استمرارية المشاريع من الحفاظ على ميزتها التنافسية.

دراسة مفتن، هدى ابراهيم، وخضير، أرادن حاتم. (1202). دور ريادة الأعمال في تحقيق التنمية المصرفية المستدامة: دراسة استطلاعية لعينة من المصارف العراقية.

هدفت الدراسة إلى تحديد دور ريادة الأعمال في التنمية المصرفية المستدامة من خلال أبعادها المتمثلة في (الإبداع والابتكار، المخاطرة، المبادرة والاستباقية) وتم التعبير عن التنمية المصرفية المستدامة بأبعادها (الاستدامة الاقتصادية، الاستدامة الاجتماعية، الاستدامة البيئية)، واعتمدت الدراسة على المنهج الوصفي التحليلي من خلال الاستبانة التي أعدت لهذا الغرض ووزعت على عينة مؤلفة من (441) فردا يمثلون مدراء الأقسام والشعب في المصارف المبحوثة فضلا عن المقابلات والملاحظات المهمة.. كما توصلت الدراسة إلى مجموعة من الاستنتاجات من أهمها أن هنالك فهم واضح لإدارات المصارف عينة البحث بأبعاد ريادة الأعمال وأبعاد التنمية المصرفية المستدامة وهذا يعد مؤشر على إدراك الإدارة المصرفية لتبني ريادة الأعمال في دعم التنمية المصرفية المستدامة. وأوصت الدراسة بضرورة استثمار العلاقة الإيجابية بين ريادة الأعمال والتنمية المصرفية المستدامة في عينة البحث من أجل زيادة الاهتمام بالبيئة والإفادة منها في تحسين سمعة المصرف.

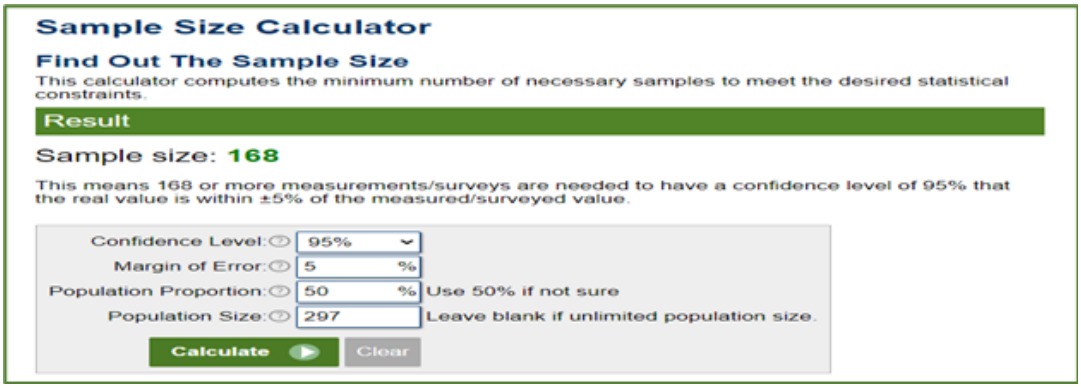
الفصل الثالث: الاجراءات المنهجية للدراسة

- **منهجية الدراسة:**

اعتمدت الدراسة على المنهج الوصفي التحليلي في جمع البيانات اللازمة لمتطلبات الدراسة من خلال الاستبانة لجمع البيانات ومن ثم تفسير وتحليل البيانات المتحصل عليها واستخلاص النتائج منها.

- **مجتمع وعينة الدراسة**

تمثل مجتمع الدراسة في جميع العاملين والمنتسبين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ والبالغ عددهم (792) موظف واعتمد الباحث على موقع (ten.rotaluclaC) لتحديد حجم العينة، وقد تم تحديدها وفقاً للشكل التالي:



وبناء عليه فقد بلغ الحد الأدنى لعينة الدراسة لكي تكون ممثلة تمثيلا صحيحا لمجتمع الدراسة (861) فرد وقام الباحث من خلال أسلوب العينة العشوائية البسيطة بجمع بيانات الدراسة عن طريق استمارة الاستبيان الإلكتروني التي تم توزيعها على أفراد مجتمع الدراسة وبلغ عدد العينة 962 عامل من العاملين في الهيئة الاتحادية للهوية والجنسية

والجمارك وأمن المنافذ وهو رقم أكبر من الحد الأدنى المطلوب مما يوضح أن عينة الدراسة تمثل المجتمع تمثيلا صحيحاً

- **أداة الدراسة**

تكون الاستبيان من خصائص العينة وعبارات محاور الدراسة (محور واقع ريادة الخدمات، ومحور استدامة ريادة الخدمات) وتضمن 03 عبارة واستخدم مقياس ليكرت الخماسي في الإجابة عن أسئلة محاور الدراسة

جدول (1) مستويات الاستجابة على عبارات أداة الدراسة

المستوي	الدرجة
منخفض جداً	1.79-1
منخفض	2.95-1.8
متوسط	3.93-2.06
مرتفع	4.19-3.04
مرتفع جداً	5.00-4.20

- **الأساليب الإحصائية**

استخدم البحث برنامج SSPS من خلال الأساليب الآتية:

- معامل الفاكرونباخ لقياس ثبات أداة الدراسة

- معامل الارتباط لتحديد مستوى الاتساق الداخلي، وصدق أداة الدراسة.

- النسب والتكرارات لوصف خصائص عينة الدراسة.

- الوسط الحسابي والانحراف المعياري لوصف مستوى استجابة أفراد عينة الدراسة لعبارات أداة الدراسة.

- اختبار (t) واختبار تحليل التباين الأحادي (AVONA) للتعرف على الفروق في استجابة أفراد عينة الدراسة التي تعزي للخصائص الشخصية

- **صدق أداة الدراسة Validity:**

تم حساب صدق عبارات استمارة الاستبيان عن طريق تحديد مستوي التجانس الداخلي

مـن خلال التعـرف علـى الدلالـة الإحصائيـة لمعـاملات الارتبـاط بيرسـون بيـن درجـة العبـارة والدرجـة الكليـة للمحـور الـذي تنتمـي إليـه العبـارة وجـاءت النتائـج كمـا يلـي

جدول (2) معاملات الارتباط لعبارات أداة الدراسة

الفقرة	الارتباط	الدلالة	الفقرة	الارتباط	الدلالة
واقع ريادة الخدمات					
1	0.875 **	0.000	9	0.925 **	0.000
2	0.839 **	0.000	10	0.776 **	0.000
3	0.868 **	0.000	11	0.869 **	0.000
4	0.842 **	0.000	12	0.835 **	0.000
5	0.907 **	0.000	13	0.912 **	0.000
6	0.922 **	0.000	14	0.892 **	0.000
7	0.912 **	0.000	15	0.910 **	0.000
8	0.917 **	0.000	-----	-----	-----
استدامة ريادة الخدمات					
1	0.926 **	0.000	9	0.956 **	0.000
2	0.933 **	0.000	10	0.874 **	0.000
3	0.930 **	0.000	11	0.944 **	0.000
4	0.931 **	0.000	12	0.941 **	0.000
5	0.920 **	0.000	13	0.898 **	0.000
6	0.914 **	0.000	14	0.894 **	0.000
7	0.943 **	0.000	15	0.951 **	0.000
8	0.960 **	0.000	-----	-----	-----

يتبين أن جميع عبارات أداة الدراسة دالة إحصائيا عند 10.0 وهذا يدل أن الأداة ذات معدل صدق مرتفع وصالحة لأغراض الدراسة.

ثبات أداة الدراسة ytilibaileR:

جدول (3) ثبات أداة الدراسة

المحور	العدد	ألفا كرونباخ
واقع ريادة الخدمات	15	0.977
استدامة ريادة الخدمات	15	0.988
إجمالي	30	0.991

يتبين أن قيمة معامل الثبات ahplA وهي أكبر من 7.0 لجميع محاور استمارة الاستبيان مما يؤكد على صلاحية وارتباط عبارات محاور استمارة الاستبيان وارتفاع مستوي ثبات أداة الدراسة مما يسمح باستخدام الأداة لغرض الدراسة.

الفصل الرابع: الإطار التطبيقي

نتائج الدراسة

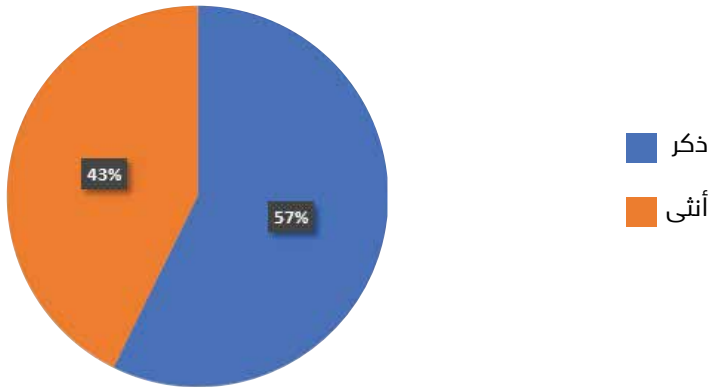
- **أولا: خصائص العينة**
- **ثانيا: الإجابة عن أسئلة الدراسة**

- **أولا: خصائص العينة**

جدول (4) وفق النوع

الفئات	ك	%
ذكر	154	57.2
أنثي	115	42.8
الإجمالي	269	100

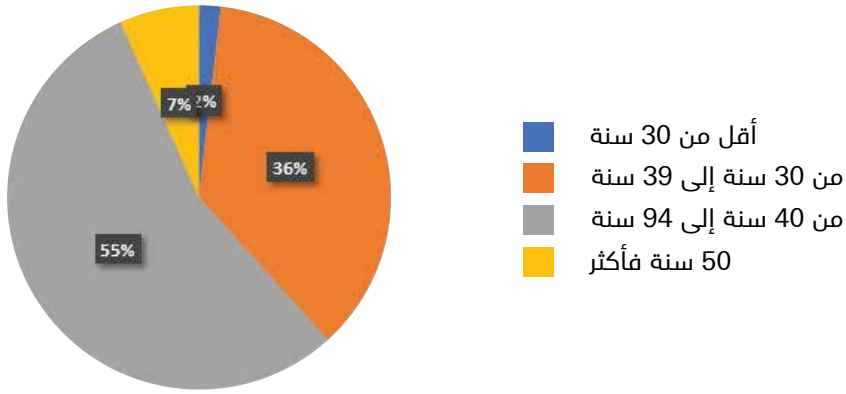
شكل (1) وفق النوع



جدول (5) وفق العمر

الفئات	ك	%
أقل من 30 سنة	5	1.9
من 30 سنة إلى 93 سنة	98	36.4
من 40 سنة إلى 49 سنة	148	55
50 سنة فأكثر	18	6.7
الاجمالي	269	100

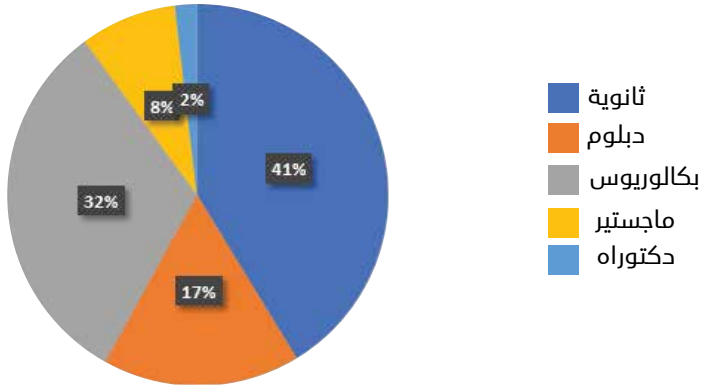
شكل (2) وفق العمر



جدول (6) وفق المؤهل العلمي

الفئات	ك	%
ثانوية	111	41.3
دبلوم	45	16.7
بكالوريوس	86	32
ماجستير	22	8.2
دكتوراه	5	1.9
الاجمالي	269	100

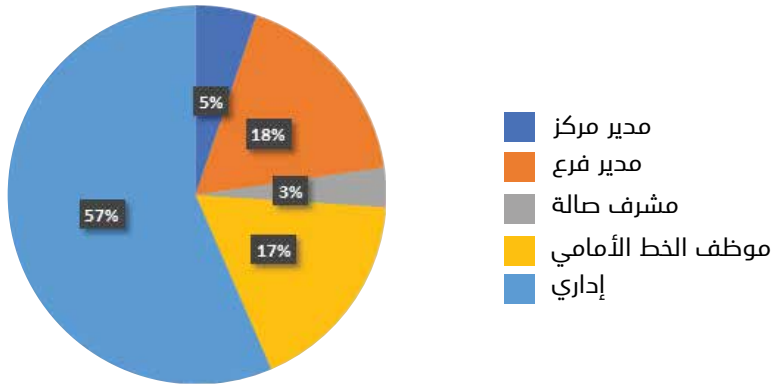
شكل (3) وفق المؤهل العلمي



جدول (7) وفق المسمى الوظيفي

الفئات	ك	%
مدير مركز	14	5.2
مدير فرع	47	17.5
مشرف صالة	9	3.3
موظف الخط الأمامي	47	17.5
دكتوراه	152	56.5
الاجمالي	269	100

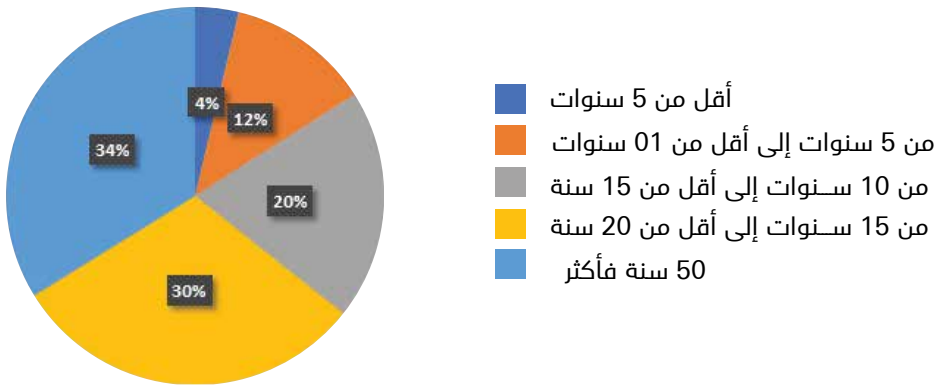
شكل (4) وفق المسمى الوظيفي



جدول (8) وفق عدد سنوات الخبرة

الفئات	ك	%
أقل من 5 سنوات	10	3.7
من 5 سنوات الي أقل من 10 سنوات	47	17.5
من 10 سنوات إلى أقل من 15 سنة	9	3.3
من 15 سنة إلى اقل من 20 سنة	47	17.5
20 سنة فأكثر	152	56.5
الاجمالي	269	100

شكل (5) وفق عدد سنوات الخبرة



ثانيا: الإجابة عن أسئلة الدراسة

نتائج الإجابة عن السؤال الأول للدراسة والذي ينص على «ما واقع ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ؟»

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية والانحرافات المعيارية لعبارات محور واقع ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ وللمحور ككل وجاءت النتائج كما يلي:

جدول (9) عبارات واقع ريادة الخدمات

الفئات	المتوسط	الانحراف	الترتيب	الموافقة
تقوم الهيئة باستخدام الأساليب الحديثة التي تساهم في زيادة جودة الخدمات المقدمة	4.301	1.830	1	مرتفع جدا
تهتم الهيئة بالتعرف على اراء العملاء في مستوى الخدمات المقدمة	4.275	1.099	3	مرتفع جدا
تعمل الهيئة على تطوير الخدمات المقدمة للعملاء بصفة دورية ومستمرة	4.283	1.069	2	مرتفع جدا
تشجع الهيئة الموظفين على الاشتراك في الدورات والبرامج التدريبية وتمنحهم المكافآت والحوافز	3.762	1.472	13	مرتفع
تقوم الهيئة بالعمل على إيجاد حلول لمشكلات ومقترحات المتعاملين في أسرع وقت ممكن	4.071	1.181	8	مرتفع
تهتم الهيئة بمتابعة التغيرات والتطورات في احتياجات وطلبات العملاء بصفة دورية ومستمرة	4.115	1.168	5	مرتفع
تهتم الهيئة بإجراء تقييم دوري لكافة الخدمات التي تقوم بتقديمها للعملاء	4.108	1.172	6	مرتفع
تهتم الهيئة بوضع الخطط والاستراتيجيات التي يمكن من خلالها تنفيذ رؤية ورسالة الهيئة بكفاءة وفاعلية	4.182	1.106	4	مرتفع
تهتم الهيئة بتوفير البنية التحتية التكنولوجية التي تتناسب مع الخدمات المقدمة للعملاء	4.086	1.151	7	مرتفع

يشجع نظام الحوافز المطبق في الهيئة الموظفين على أداء أعمالهم بالكفاءة والفعالية المطلوبة	3.446	1.524	15	مرتفع
تهتم الهيئة بتقييم مستويات أداء العاملين بصفة مستمرة	3.732	1.407	14	مرتفع
تهتم الهيئة بتوفير البيئة المادية المناسبة للعمل (الإضاءة، المكاتب، التكييف، الأدوات المكتبية)	3.996	1.265	10	مرتفع
تشجع الهيئة العاملين على التعاون مع بعضهم البعض في انجاز المهام المطلوبة	4.007	1.255	9	مرتفع
تهتم الهيئة بوجود علاقات جيدة بين الرؤساء والمرؤوسين لزيادة جودة العمل	3.993	1.307	11	مرتفع
تعمل الهيئة على تكوين فرق عمل لتشجيع العاملين على المشاركة في اتخاذ القرار	3.952	1.276	12	مرتفع

تم ترتيب عبارات محور واقع ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (تقوم الهيئة باستخدام الأساليب الحديثة التي تساهم في زيادة جودة الخدمات المقدمة) هي أكثر العبارات أهمية بقيمة 103.4 وانحراف معياري 830.1 وبدرجة موافقة مرتفعة جدا بينما كانت العبارة (يشجع نظام الحوافز المطبق في الهيئة الموظفين على أداء أعمالهم بالكفاءة والفعالية المطلوبة) هي أقل العبارات اهمية بقيمة 644.3 وانحراف معياري 425.1 وبدرجة موافقة مرتفعة وعند دراسة عبارات واقع ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ تبين أن ثلاث عبارات في مستوى الموافقة المرتفع جدا وإثنى عشر في مستوي الموافقة المرتفع مما يوضح وجود مستوي مرتفع من تطبيق ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ حيث بلغت قيمة المتوسط الحسابي

لعبارات واقع ريادة الخدمات 120.4 بانحراف معياري 332.1 وهو ما يجيب عن السؤال الأول للدراسة

نتائج الإجابة عن السؤال الثاني للدراسة والذي ينص على « ما مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ؟»

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية والانحرافات المعيارية لعبارات محور استدامة ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ وللمحور ككل وجاءت النتائج كما يلي:

جدول (10) عبارات استدامة ريادة الخدمات

الفئات	المتوسط	الانحراف	الترتيب	الموافقة
تعمل الهيئة على زرع ثقافة التميز في تقديم الخدمات لدي الموظفين	4.022	1.246	8	مرتفع
تقوم الهيئة بتدريب الموظفين على أحدث الأساليب المستخدمة في تقديم الخدمات	3.952	1.285	10	مرتفع
تقوم الهيئة بعمل استبيانات منتظمة للتعرف على اراء العملاء في الخدمات المقدمة	4.026	1.244	7	مرتفع
تهتم الهيئة بتجديد خدماتها بصفة مستمرة ودورية	4.059	1.241	3	مرتفع
تقوم الهيئة باستخدام الأساليب التكنولوجية الحديثة لزيادة مستوى جودة الخدمات	4.156	1.125	1	مرتفع

تهتم الهيئة باستخدام أساليب التقييم التي تساهم في تحديد مستوى جودة الخدمات المقدمة للعملاء	4.104	1.161	2	مرتفع
تهتم الهيئة بتقوية العلاقات مع الجهات المساعدة في تقديم الخدمة	4.048	1.204	6	مرتفع
تقوم الهيئة بالعمل على حل كافة المشكلات التي تعيق تنفيذ الأهداف الاستراتيجية بكفاءة وفاعلية	4.048	1.179	5	مرتفع
تعمل الهيئة على تكوين فرق العمل التي تساهم في زيادة جودة الخدمات المقدمة للعملاء	4.056	1.228	4	مرتفع
تمنح الهيئة مكافآت وحوافز للموظفين المبدعين التي تقدم أفكار ابتكارية تساعد في تنمية وتطوير إجراءات ونظم العمل	3.691	1.416	15	مرتفع
تهتم الهيئة بتحديث وتطوير أنظمة وإجراءات العمل	4.004	1.235	9	مرتفع
تعمل الهيئة على اطلاع الموظفين بكل ما هو جديد في مجال تقديم الخدمات	3.918	1.322	12	مرتفع
تعمل الهيئة على تشجيع الموظفين على اقتراح أفكار تساهم في تطوير نظم العمل	3.907	1.294	13	مرتفع
تعمل الهيئة على توفير الدعم الكامل للموظفين لتوفير أفضل مستوى جودة حياة ممكن	3.710	1.429	14	مرتفع

تعمل الهيئة على توفير المرونة التي تساهم في زيادة القدرة على مواكبة أي تغيرات يمكن ان تحدث في نظم العمل	3.929	1.298	11	مرتفع

تم ترتيب عبارات محور استدامة ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (تقوم الهيئة باستخدام الأساليب التكنولوجية الحديثة لزيادة مستوى جودة الخدمات) هي أكثر العبارات أهمية بقيمة 651.4 وانحراف معياري 521.1 وبدرجة موافقة مرتفعة بينما كانت العبارة (تمنح الهيئة مكافآت وحوافز للموظفين المبدعين التي تقدم أفكار ابتكارية تساعد في تنمية وتطوير إجراءات ونظم العمل) هي أقل العبارات اهمية بقيمة 196.3 وانحراف معياري 614.1 وبدرجة موافقة مرتفعة وعند دراسة عبارات استدامة ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ تبين أن جميع العبارات في مستوي الموافقة المرتفع مما يوضح وجود مستوي مرتفع من تحقيق استدامة ريادة الخدمات في مراكز إسعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ حيث بلغت قيمة المتوسط الحسابي لعبارات استدامة ريادة الخدمات 579.3 بانحراف معياري 062.1 وهو ما يجيب عن السؤال الثاني للدراسة

نتائج الإجابة عن السؤال الثالث للدراسة والذي ينص على « هل توجد فروق دالة احصائيا بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير (النوع – الخبرة –العمر- الوظيفة- المؤهل الدراسي)؟»

للإجابة عن هذا السؤال تم حساب اختبار (t) للفروق التي تعزي لمتغير النوع واختبار تحليل التباين الأحادي (AVONA) التي تعزي لمتغيرات (الخبرة –العمر- الوظيفة- المؤهل الدراسي) وجاءت النتائج كما يلي:

جدول (11) نتائج اختبار (t) للفروق التي تعزى لمتغير النوع

الفئات	العدد	المتوسط الحسابي	قيمة t	Sig

ذكر	154	58.578	2.036	0.043
أثني	115	62.626		

يتبين وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير النوع مما يبين إن هناك فروق بين الذكور والإناث من افراد عينة الدراسة في الاستجابة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين وكانت الفروق لصالح فئة الإناث مما يبين إنها الفئة الأكثر وعيا بواقع ريادة الخدمات في مراكز إسعاد المتعاملين

جدول (12) نتائج اختبار (AVONA) للفروق التي تعزى لمتغير لمتغيرات (الخبرة –العمر- الوظيفة- المؤهل الدراسي)

الخصائص	الفئات	العدد	المتوسط الحسابي	قيمة F	Sig
العمر	أقل من 30 سنة	5	53.800		
	من 30 سنة إلى 39 سنة	98	16.892		
	من 40 سنة إلى 49 سنة	148	61.892		
	50 سنة فأكثر	18	58.722		
المؤهل العلمي	ثانوية	111	57.568	2.155	0.074
	دبلوم	45	64.222		
	بكاوريوس	86	61.733		
	ماجستير	22	62.636		
	دكتوراه	5	51.200		

المسمى الوظيفي	مدير مركز	14	70.071	5.436	0.000
	مدير فرع	47	65.064		
	مشرف صالة	9	52.000		
	موظف الخط الأمامي	47	53.255		
	إداري	152	60.612		
عدد سنوات الخبرة	أقل من 5 سنوات	10	70.600	1.269	
	من 5 سنوات الى أقل من 10 سنوات	33	06.455		
	من 10 سنوات الى أقل من 15 سنوات	53	59.415		
	من 15 سنوات الى أقل من 20 سنوات	82	58.805		
	20 سنة فأكثر	91	61.000		

يتبين عدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير العمر مما يبين إن ليس هناك فروق بين فئات العمر لأفراد عينة الدراسة في الاستجابة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين

يتبين عدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير المؤهل العلمي مما يبين إن ليس هناك فروق بين فئات المؤهل العلمي لأفراد عينة الدراسة في الاستجابة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين

يتبين وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير المسمى الوظيفي مما يبين إن هناك فروق بين فئات المسمى الوظيفي لأفراد عينة الدراسة في الاستجابة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين وكانت الفروق لصالح فئة مدير المركز مما يبين إنها الفئة الأكثر وعيا بواقع ريادة الخدمات في مراكز إسعاد المتعاملين

يتبين عدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير عدد سنوات الخبرة مما يبين إن ليس هناك فروق بين فئات عدد سنوات الخبرة لأفراد عينة الدراسة في الاستجابة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين

تبين مما سبق وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغيرات (العمر، المسمى الوظيفي) وعدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغيرات (العمر، المؤهل العلمي، عدد سنوات الخبرة) وهو ما يجيب عن السؤال الثالث للدراسة

نتائج الإجابة عن السؤال الرابع للدراسة والذي ينص على « هل توجد فروق دالة احصائيا بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير (النوع – الخبرة –العمر- الوظيفة- المؤهل الدراسي)؟»

للإجابة عن هذا السؤال تم حساب اختبار (t) للفروق التي تعزي لمتغير النوع واختبار تحليل التباين الأحادي (AVONA) التي تعزي لمتغيرات (الخبرة –العمر- الوظيفة- المؤهل الدراسي) وجاءت النتائج كما يلي:

جدول (31) نتائج اختبار (t) للفروق التي تعزى لمتغير النوع

الفئات	العدد	المتوسط الحسابي	قيمة t	Sig
ذكر	154	58.149	0.267	0.109
أنثي	115	61.617		

يتبين عدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير النوع مما يبين إن ليس هناك فروق بين الذكور والاناث من افراد عينة الدراسة في الاستجابة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين

جدول (14) نتائج اختبار (AVONA) للفروق التي تعزى لمتغير لمتغيرات (الخبرة –العمر- الوظيفة- المؤهل الدراسي)

الخصائص	الفئات	العدد	المتوسط الحسابي	قيمة F	Sig
العمر	أقل من 30 سنة	5	51.600	1.726	0.162
	من 30 سنة إلى 39 سنة	98	57.296		
	من 40 سنة إلى 49 سنة	148	61.710		
	50 سنة فأكثر	18	57.500		

المؤهل العلمي	ثانوية	111	56.649	2.155	0.074
	دبلوم	45	63.556		
	بكاوريوس	86	61.233		
	ماجستير	22	62.227		
	دكتوراه	5	51.600		
المسمى الوظيفي	مدير مركز	14	69.429	5.436	0.000
	مدير فرع	47	64.511		
	مشرف صالة	9	52.000		
	موظف الخط الأمامي	47	52.064		
	إداري	152	60.613		

عدد سنوات الخبرة	أقل من 5 سنوات	10	96.100	1.269
	من 5 سنوات الى أقل من 10 سنوات	33	58.091	
	من 10 سنوات الى أقل من 15 سنوات	53	58.509	
	من 15 سنوات الى أقل من 20 سنوات	82	58.781	
	20 سنة فأكثر	91	60.571	

يتبين عدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير العمر مما يبين إن ليس هناك فروق بين فئات العمر لأفراد عينة الدراسة في الاستجابة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين

يتبين عدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير المؤهل العلمي مما يبين إن ليس هناك فروق بين فئات المؤهل العلمي لأفراد عينة الدراسة في الاستجابة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين

يتبين وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير المسمى الوظيفي مما يبين إن هناك فروق بين فئات المسمى الوظيفي لأفراد عينة الدراسة في الاستجابة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين وكانت

الفروق لصالح فئة مدير المركز مما يبين إنها الفئة الأكثر وعيا بمستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين

يتبين عدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير عدد سنوات الخبرة مما يبين إن ليس هناك فروق بين فئات عدد سنوات الخبرة لأفراد عينة الدراسة في الاستجابة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين

تبين مما سبق وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغير (المسمى الوظيفي) وعدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز إسعاد المتعاملين تعزى لمتغيرات (النوع، العمر، المؤهل العلمي، عدد سنوات الخبرة) وهو ما يجيب عن السؤال الرابع للدراسة

الفصل الخامس

النتائج والتوصيات

استنتاجات الدراسة

- **توصلت الدراسة إلى النتائج التالية:**

- وجود مستوي مرتفع من تطبيق ريادة الخدمات في مراكز سعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ وهو ما يجيب عن السؤال الأول للدراسة وتتفق هذه النتيجة عن نتيجة دراسة مرهج، وحسن (0202) وتختلف هذه النتيجة عن نتيجة دراسة بو حمادة، ونصار (6102) التي أوضحت ضعف توجه المستشفيات الحكومية السعودية بمنطقة تبوك نحو ريادة الأعمال

- وجود مستوي مرتفع من تحقيق استدامة ريادة الخدمات في مراكز سعاد المتعاملين من وجهة نظر العاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ وهو ما يجيب عن السؤال الثاني للدراسة وتتفق هذه النتيجة مع نتيجة دراسة الطائي، أحمد هادي طالب. (6102)

- وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغير النوع وكانت الفروق لصالح فئة الاناث مما يبين إنها الفئة الأكثر وعيا بواقع ريادة الخدمات في مراكز سعاد المتعاملين وتختلف هذه النتيجة عن نتيجة دراسة العمري، ومقدادي (0202) التي أوضحت عدم وجود فروق تعزى لمتغير النوع

- وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغير المسمى الوظيفي وكانت الفروق لصالح فئة مدير المركز مما يبين إنها الفئة الأكثر وعيا بواقع ريادة الخدمات في مراكز سعاد المتعاملين

- عدم وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغيرات (العمر، المؤهل العلمي، عدد سنوات الخبرة) وتتفق هذه النتيجة مع نتيجة دراسة العمري، ومقدادي (0202) التي أوضحت وجود عدم فروق تعزى لمتغير العمر في حين تختلف عنها في إنها أوضحت وجود فروق تعزي تعزى لمتغيرات (المؤهل العلمي، عدد سنوات الخبرة)

- وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة حول واقع ريادة الخدمات

في مراكز سعاد المتعاملين تعزى لمتغيرات (العمر، المسمى الوظيفي) وعدم وجود فروق ذات دلالة إحصائية عند مستوى 50.0 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغيرات (العمر، المؤهل العلمي، عدد سنوات الخبرة) وهو ما يجيب عن السؤال الثالث للدراسة

- وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغير المسمى الوظيفي وكانت الفروق لصالح فئة مدير المركز مما يبين إنها الفئة الأكثر وعيا بمستوى استدامة ريادة الخدمات في مراكز سعاد المتعاملين
- عدم وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغيرات (النوع، العمر، المؤهل العلمي، عدد سنوات الخبرة)
- وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة حول مستوى استدامة ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغير (المسمى الوظيفي) وعدم وجود فروق ذات دلالة إحصائية عند مستوى 0.05 بين استجابات عينة الدراسة حول واقع ريادة الخدمات في مراكز سعاد المتعاملين تعزى لمتغيرات (النوع، العمر، المؤهل العلمي، عدد سنوات الخبرة) وهو ما يجيب عن السؤال الرابع للدراسة.

العلاقة بين نتائج الدراسة والدراسات السابقة:

في ضوء النتائج الإحصائية التي توصلت إليها الدراسة يتبدّى بوضوح وجود مستوى مرتفع من تطبيق «ريادة الخدمات» في مراكز سعادة المتعاملين، ومتوسط عام بلغ (4.021) لانعكاس واقع الريادة، مقابل مستوى مرتفع أيضاً لاستدامتها بمتوسط (3.975)، وهو ما يدعم أطروحة الدراسة الرئيسة بأن تبنّي ممارسات ريادية ممنهجة داخل الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ يرتبط بقدرة المؤسسة على تثبيت مزاياها وتحويل التحسينات التشغيلية إلى مكاسب مستدامة، وتضع هذه النتيجة الدراسة في حالة اتساق قوي مع ما خلصت إليه دراسات سابقة ربطت بين التوجهات الريادية والميزة التنافسية المستدامة وجودة الخدمة، إذ تتوافق مباشرة مع نتائج الطائي (6102) حول دور الاستراتيجيات الريادية في تعظيم الاستدامة، كما تنسجم مع مرهج وحسن (2020) اللذين أكّدا أن تبني الريادة يرفع جودة الخدمات الفندقية/الخدمية، في المقابل تُظهر الدراسة فارقاً سياقياً مهمّاً مع بو حمادة ونصار (2016) الذين سجّلوا ضعف التوجّه الريادي في مستشفيات حكومية بمنطقة تبوك؛ ويُحتمل أن يعود هذا التباين إلى

خصوصية البيئة المؤسسية والخطط الرقمية والتنظيمية في الهيئة محلّ التطبيق التي دفعت مؤشرات الريادة والاستدامة إلى مستويات مرتفعة مقارنة ببيئات خدمية أخرى. هذا الاتساق/التغاير مع الأدبيات رصده الباحث صراحة ضمن «استنتاجات الدراسة» ما يمنح الربط مع الدراسات السابقة أساساً توثيقياً داخلياً صلباً، وعند تفكيك بنود المحورين على مستوى العبارة تتضح علاقة عضوية بين ما رصدته الدراسة وبين ما شدّدت عليه الأدبيات من أن الابتكار والتقنيات الحديثة هما محرّكا الجودة والاستدامة، فالعبارة الأعلى وزناً في محور «واقع ريادة الخدمات» كانت «استخدام الأساليب الحديثة التي تساهم في زيادة جودة الخدمات» (متوسط 103.4)، وفي محور «استدامة ريادة الخدمات» برزت «استخدام الأساليب التكنولوجية الحديثة لزيادة مستوى جودة الخدمات» كالأعلى أهمية (651.4)، وهذه الصورة الدقيقة تُجسّد عملياً ما تشير إليه دراسات التوجه الريادي من أن الإبداع والسبْق التقني هما القلب النابض للأثر المستدام وتفسّر لماذا جاءت الدرجات الكلية مرتفعة على الاستدامة؛ فحين تتركّز الريادة على تحديث الأساليب والمنصات ويكون من الأسهل تحويل المكاسب إلى ممارسات معيارية دائمة، وتزداد أهمية هذا الربط حين نتذكّر ما توصّل إليه علي وآخرون (2020) من أن «الاندفاع نحو المخاطرة» قد لا يرتبط دائماً بالأداء المستدام، بينما يرتبط به الإبداع والاستباقية؛ وهو ما يتماشى ضمنياً مع طبيعة أداة الدراسة التي شدّدت—بحسب نتائج البنود—على التحديث التقني والتقويم والتحسين المستمر أكثر من تشجيع المخاطرة كقيمة مستقلة، فانعكست هذه الأولويات على ارتفاع مؤشر الاستدامة، وبذلك تغدو العلاقة بين النتائج والحقل المعرفي علاقة دعمٍ تأكيدي: التكنولوجيا والابتكار هما وسيطا الأثر من الريادة إلى الاستدامة في السياقات الحكومية الخدمية، في المقابل تكشف الدراسة عن نقطة افتراق جزئية مع بعض الطروحات التطبيقية في الأدبيات المتعلقة بـ«تمكين رأس المال البشري» بوصفه شرطاً لازماً للاستدامة وذلك من خلال انخفاض نسبي في أوزان العبارات المرتبطة بالحوافز مقارنة بغيرها؛ إذ جاءت عبارة «يشجع نظام الحوافز...» كأدنى العبارات وزناً في محور الواقع (3.446)، وعبارة «تمنح الهيئة مكافآت وحوافز للموظفين المبدعين...» كالأدنى في محور الاستدامة (196.3)، رغم بقائهما ضمن مستوى «موافقة مرتفع». قراءة هذه المفارقة في ضوء الأدبيات التي تُبرز دور الحوافز والتنظيمات الداعمة للابتكار—ومنها أعمال تناولت «عوامل النجاح المؤثرة في استدامة المنشآت الصغيرة والمتوسطة»—تشير إلى أن البيئة التقنية والتنظيمية القوية في الهيئة نجحت في دفع

الريادة والاستدامة إلى مستويات عالية حتى مع حيّزٍ قابل للتحسين في أنظمة التحفيز، وعليه تُفهم النتائج على أنها «اتساق مع الأدبيات» في الجوهر (تقنية/ابتكار/استدامة) مع إبراز «فجوة سياستيه» يمكن سدّها لتعظيم الأثر المستدام عبر مواءمة الحوافز مع الأهداف الريادية، وهو ما ينسجم أيضاً مع توصيات الدراسة الداعية إلى توسيع البحوث التطبيقية حول عوامل الريادة وأثرها على الأداء والإنتاجية في مؤسسات دولة الإمارات العربية المتحدة، أما على مستوى المتغيرات الديموغرافية والتنظيمية، فتُظهر النتائج علاقة دقيقة ومعقّدة مع ما أورده التراث البحثي: فقد برزت فروق دالة لصالح الإناث في «واقع ريادة الخدمات»—وهي نتيجة تختلف عن العمري ومقدادي (2020) الذين لم يجدوا فروقاً تُعزى للنوع—بينما توافقت الدراسة معهم في عدم وجود فروق تُعزى للعمر، في المقابل اختلفت نتائجنا مع ما أفاد به العمري ومقدادي بشأن المؤهل والخبرة، حيث لم تظهر فروق دالة في هذه الدراسة لأي منهما، وهذا التمايز يلفت إلى أن الوعي الريادي قد يتأثر بعوامل ثقافية/تنظيمية محلية (تمكين العاملات، أساليب العمل، توزيع الأدوار) أكثر من تأثره بخصائص بشرية ثابتة كالعمر أو سنوات الخبرة، في سياقٍ حكومي رقمي عالي التنظيم، وبصورة متسقة تماماً مع منطق الأدبيات التي تُظهر تفاوتاً في تبنّي الممارسات الريادية باختلاف الموقع الوظيفي، وجدت الدراسة فروقاً دالة لصالح «مدير المركز» في كلٍّ من الواقع والاستدامة ما يعكس قرب هذه الفئة من دائرة صنع القرار ومنظومات التخطيط والتقويم وبالتالي إدراكاً أعلى للمبادرات الريادية والاستدامة الجارية، وهذا النمط—تباينٌ بحسب «المسمى الوظيفي» وثبات نسبي عبر «العمر/الخبرة/المؤهل»—يُبرز أن محركات الوعي الريادي أكثر «بنائية-مؤسسية» من كونها «فردية-سكانية»، وهو تفسير يتوافق مع الأطر النظرية التي تربط الريادة المؤسسية بالبنى التنظيمية وآليات الحوكمة، وتتوطد هذه القراءة التكاملية حين نضع النتائج في سياق تصميم الدراسة وعينتها (269 موظفاً/موظفة من الهيئة)؛ فحجم العينة وتنوّعها يدعمان صلابة الاستنتاجات داخل الإطار المؤسسي محل الدراسة، كما يمنحان مصداقية أكبر للربط بين «التحديث التقني + آليات التقييم والتحسين» من جهة، و«الاستدامة» من جهة أخرى، مع إبراز أن تعزيز منظومات الحوافز وتمكين غير المديرين من موطئ قدمٍ أقوى في دوائر التخطيط قد يضيق الفجوة الإدراكية بين المستويات الوظيفية ويرفع سقف الاستدامة أكثر، وتلتقي هذه الخلاصة مع توصيات الباحث بالتوسّع في الدراسات التطبيقية داخل مؤسسات الدولة لتحديد العوامل الأكثر فعالية في نقل الريادة من مبادرات متفرقة إلى «نُسق مؤسسية مستدامة» بما يعمّق الأثر على الأداء والإنتاجية والخدمة العامة، وبهذا المعنى فإن علاقة نتائج الدراسة بالأدبيات ليست علاقة «تأكيدٍ

تجريبي» فحسب، بل تقدم أيضاً «مثاراً نظرياً» يُغني النقاش حول وزن التقنية والحوكمة مقابل الحوافز في بناء الاستدامة الريادية في القطاع الحكومي.

التوصيات

فيما يلي مجموعة من التوصيات التي يمكن أن تساعد في تعزيز ريادة الخدمات واستدامتها:

- العمل على توفير البرامج والدورات التدريبية للعاملين في مراكز سعاد المتعاملين للحفاظ على المستوى المتميز من واقع ريادة الخدمات في هذه المراكز من خلال تطبيق التجارب والنماذج العالمية والتي تتفق مع بيئة وطبيعة العمل في الهيئة الاتحادية
- العمل على الاستفادة من تجربة تطبيق ريادة الخدمات في مراكز سعاد المتعاملين في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ في كافة المؤسسات العاملة بدولة الامارات العربية من خلال نشر التجربة وطرق تنفيذها وتطويرها وفق طبيعة عمل كافة المؤسسات العاملة بدولة الامارات العربية
- توفير البنية التحتية التي تساهم في زيادة قدرة الشركات والمؤسسات على تحقيق استدامة في ريادة الخدمات من خلال الاهتمام بتوفير البنية التكنولوجية والفنية والبشرية التي تساهم في تحفيف الاستدامة المطلوبة
- ضرورة العمل على زيادة مستوي وعي الشركات والمؤسسات بدولة الامارات العربية بأهمية تطبيق ريادة الخدمات والعمل على توفير كافة الإمكانيات والاحتياجات التي تسهل تحقيق ذلك من خلال المؤتمرات والندوات التي توضح كيفية تطبيق ريادة الخدمات وأهميتها والمميزات والفوائد التي تعود على المؤسسات من تطبيقها.

المقترحات

التوسع في إجراء الدراسات والأبحاث المتعلقة بعوامل ريادة الخدمات في كافة المنشآت والمؤسسات العاملة بدولة الإمارات العربية المتحدة وأثرها على مستويات الأداء والإنتاجية

التوسع في إجراء الدراسات والأبحاث المتعلقة بمستوى استدامة ريادة الخدمات في كافة المنشآت والمؤسسات العاملة بدولة الامارات العربية المتحدة وأثرها على مستويات الأداء والانتاجية.

المراجع:

أولاً: المراجع العربية

1. أبو النصر، مدحت ومحمد، ياسمين. (2017). التنمية المستدامة مفهومها – أبعادها – مؤشراتها. د.ط، القاهرة: المجموعة العربية للتدريب والنشر.
2. أبو حمادة، عبد الموجود وعبد الله، نصار وحمدي، جابر محمد. (2016). ريادة الأعمال وجودة الخدمات الصحية داخل المستشفيات الحكومية بمنطقة تبوك. مجلة مركز صالح عبد الله كامل للاقتصاد الاسلامي، ع.02، ص. 991 – 552.
3. أحمد، دروم. (2019). الإبداع ريادة الأعمال والتنمية الاقليمية (المحلية) المستدامة: دراسات ميدانية وتجارب رائدة. منشورات مخبر الطرق الكمية في العلوم الاقتصادية وعلوم إدارة الأعمال وتطبيقاتها من أجل التنمية المستدامة.
4. البارودي، علي سيد عبد الرحمن. (2017). دراسة تحليلية لأثر تأكيد تقارير الاستدامة على التنمية المستدامة لمنشآت الأعمال. المجلة العلمية للدراسات التجارية والبيئية، ع.4، ص. 316- 356.
5. بن البشير، عبد الوهاب. (2022). التنمية المستدامة «الأسباب والأهداف. مجلة البيئة والتنمية المستدامة وصحة الإنسان، ع.1، ص. 73-86.
6. خطاب، أحمد ومحمد، حازم وحسانين، محمد. (2020). فاعلية ريادة الاعمال في تعزيز استراتيجية التنمية المستدامة في ضوء رؤية مصر 2030، 11(1)، ج2، ص. 473- 518.
7. الخطيب، آيات عليان العطيات. (2023). أثر عوامل النجاح الحرجة على استدامة المشاريع الريادية في الأردن. رسالة ماجستير، جامعة البلقاء.
8. صحراوي، عبد الرزاق. (2021). مبادئ التنمية المستدامة في القانون الدولي للبيئة. رسالة دكتوراه، جامعة باتنة -1 الحاج لخضر، الجزائر.
9. الطائي، أحمد هادي طالب. (2016). دور تبني الاستراتيجيات الريادية وتأثيرها في تحقيق الميزة التنافسية المستدامة: دراسة استطلاعية على شركة بغداد للمشروبات الغازية المساهمة المختلطة. مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية، ع.8، ص. 136 - 160.
10. العبادي، هاشم والحدراوي، حامد. (2011). الريادة الإستراتيجية ودورها في صياغة استراتيجية التسويق الريادي في منظمات الأعمال: دراسة تطبيقية في معمل بيبسي

الكوفة. مجلة القادسية للعلوم الإدارية والاقتصادية، ع.1، ص. 8 - 35.

11. العتيبي، منصور وموسى، محمد. (2015). الوعي بثقافة ريادة الأعمال لدى طلاب جامعة نجران واتجاهاتهم نحوها: دراسة ميدانية. مجلة التربية، ع.162، ص. 615 - 670.

12. علي، رحاب ومحمود، عبد الله وحامد، عبد السلام. (2020). أثر التوجه الريادي على الأداء المستدام: دراسة على عينة من المؤسسات الخدمية بولاية الخرطوم. مجلة كلية التجارة العلمية، ع.9، ص. 79 - 101.

13. العمري، سامر ومقدادي، يونس. (2020). أثر استراتيجيات الريادة في تحقيق الاستدامة للمشاريع الصغيرة في مدينة إربد. رسالة ماجستير غير منشورة. جامعة عمّان العربية، عمّان.

14. عياش، وجدان والجوازنة، بهجت. (2021). Assessing the Success Factors and their Impact on Sustainability of the Small and Medium Entrepreneurial Enterprises in Mafraq Governorate (رسالة ماجستير). جامعة آل البيت، المفرق.

15. غازي، سمر والجزار، فاروق. (2020). دور ريادة الأعمال في تحقيق أهداف التنمية المستدامة مع الإشارة إلى الواقع المصري. مجلة التجارة والتمويل، عدد خاص، ص. 1 - 35.

16. فتيحة، بن حاج جيلالي مغراوة. (2017). التنمية المستدامة بين الطرح النظري والواقع العملي: دراسة الاستراتيجية العربية المقترحة للتنمية المستدامة لما بعد عام 2005. مجلة الإدارة والتنمية للبحوث والدراسات، ع.11 ص. 152 - 167.

17. لطفي، خالد منذر موسى. (2019). استراتيجيات الريادة وجودة الخدمات الفندقية: دراسة في فنادق العاصمة عمان. رسالة ماجستير، جامعة البلقاء التطبيقية، السلط.

18. محمد، عوض ومحمود، أشرف. (2014). قياس مستوى ريادة الأعمال لدى طلاب جامعة الطائف ودور الجامعة في تنميتها. مجلة البحث العلمي في التربية، ع.15، ص. 549 - 599.

19. مرهج، منذر وحسن، باسم. (2020). دور الريادة في تعزيز جودة الخدمة الفندقية: دراسة ميدانية على فنادق الأربع والخمس نجوم في مدينة اللاذقية. مجلة جامعة تشرين للبحوث والدراسات العلمية - سلسلة العلوم الاقتصادية والقانونية، ع.3، ص. 437 - 457.

20. مفتن، هدى وخضير، أرادن. (2021). دور ريادة الاعمال في تحقيق التنمية المصرفية المستدامة: دراسة استطلاعية لعينة من المصارف العراقية. مجلة الإدارة والاقتصاد، ع.129، ص. 1 - 21.

21. نخلة، رأفت ومسعد، رانيا (2022). معايير الاستدامة وتأثيرها على التصميم الداخلي للفنادق الخضراء، مجلة الجمعية العربية للحضارة والفنون الإسلامية، ع.2، ص. 58-69.

22. نعمة، نغم والورد، حمزة. (2022) تقييم التوجه الريادي في انجاح المشاريع الصغيرة والمتوسطة -تجربة الاردن وماليزيا انموذجاً-. مجلة الريادة للمال والأعمال، ع.1، ص. 13-21.

23. والي محمد فوزي رياض. (2023). دور التكنولوجيا الحديثة في تحقيق التنمية المستدامة في ضوء رؤية مصر 2030. المجلة الدولية للعلوم التربوية والإنسانية المعاصرة، ع.1، ص. 1-20.

ثانياً: المراجع الأجنبية

1. Afshari, H., Agnihotri, S., Searcy, C., and Jaber, M. Y. (2022). Social eht ni noitacilppA htiw weiveR evisneherpmoC A :srotacidnI ytilibaniatsuS .noitpmusnoC dna noitcudorP elbaniatsuS .rotceS ygrenE

2. Assembly, G. (2015). Sustainable development goals. In: SDGs, Transforming .29-our world: the 2030, (82), 1

3. Jumah, P. K., Githui, T., and Kweyu, M. (2022). An Exploratory Study on the Role of Feasibility Study on Sustainability of Business in Kenya: A Case of Supermarkets in Nairobi County. Journal of Finance and Accounting .70-57 ,(1)6 ,

4. Rachman, M. W.; Parvin, L. and Jia Ji., «Women entrepreneurship development in Bangladesh: What are the challenges ahead? African Journal of Business Management. 6)11), 2011, 38623871-.

5. Reza,Amin,et.al (2016):Providing Functional Model for Developing Entrepreneurship, International Journal of Development Studies. 8(1), 89105-.

الملاحق

استمارة الاستبيان

استدامة ريادة الخدمات في مراكز سعاد المتعاملين / دراسة تطبيقية على الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ

الأستاذ / ة:

تحية طيبة وبعد،

يستهدف الاستبيان التعرف على استدامة ريادة الخدمات في مراكز إسعاد المتعاملين / دراسة تطبيقية على الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ وأرجو من سيادتكم الإجابة على أسئلة الاستبيان بدقة وموضوعية. علماً بأن البيانات التي سيتم الحصول عليها من خلال إجاباتكم سوف تستخدم لأغراض البحث العلمي فقط وستتم المحافظة عليها بكامل السرية.

ولكم جزيل الشكر والامتنان على حسن تعاونكم

أولا: الخصائص الشخصية:

الجنس:

- ذكر
- انثي

العمر:

أقل من 03 سنة

من 03 سنة إلى 93 سنة

من 04 سنة إلى 94 سنة

05 سنة فأكثر

المؤهل العلمي:

- ثانوية
- دبلوم
- بكالوريوس
- ماجستير
- دكتوراه

المسمى الوظيفي:

- مدير مركز
- مدير فرع
- مشرف صالة
- موظف الخط الأمامي
- إداري

عدد سنوات الخبرة الوظيفية

- أقل من 5 سنوات
- من 5 سنوات الي أقل من 10 سنوات
- من 01 سنوات إلى أقل من 15 سنة
- من 15 سنة إلى اقل من 20 سنة
- 20 سنة فأكثر

ثانيا: محاور الاستبيان

محور عوامل ريادة الخدمات

م	العبارات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تقوم الهيئة باستخدام الأساليب الحديثة التي تساهم في زيادة جودة الخدمات المقدمة					
2	تهتم الهيئة بالتعرف على اراء العملاء في مستوى الخدمات المقدمة					
3	تعمل الهيئة على تطوير الخدمات المقدمة للعملاء بصفة دورية ومستمرة					

4	تشجع الهيئة الموظفين على الاشتراك في الدورات والبرامج التدريبية وتمنحهم المكافآت والحوافز					
5	تقوم الهيئة بالعمل على إيجاد حلول لمشكلات ومقترحات المتعاملين في أسرع وقت ممكن					
6	تهتم الهيئة بمتابعة التغيرات والتطورات في احتياجات وطلبات العملاء بصفة دورية ومستمرة					
7	تهتم الهيئة بإجراء تقييم دوري لكافة الخدمات التي تقوم بتقديمها للعملاء					
8	تهتم الهيئة بوضع الخطط والاستراتيجيات التي يمكن من خلالها تنفيذ رؤية ورسالة الهيئة بكفاءة وفاعلية					
9	تهتم الهيئة بتوفير البنية التحتية التكنولوجية التي تتناسب مع الخدمات المقدمة للعملاء					
10	يشجع نظام الحوافز المطبق في الهيئة الموظفين على أداء أعمالهم بالكفاءة والفعالية المطلوبة					
11	تهتم الهيئة بتقييم مستويات أداء العاملين بصفة مستمرة					
12	تهتم الهيئة بتوفير البيئة المادية المناسبة للعمل (الإضاءة، المكاتب، التكييف، الأدوات المكتبية)					

13	تشجع الهيئة العاملين على التعاون مع بعضهم البعض في انجاز المهام المطلوبة					
14	تهتم الهيئة بوجود علاقات جيدة بين الرؤساء والمرؤوسين لزيادة جودة العمل					
15	تعمل الهيئة على تكوين فرق عمل لتشجيع العاملين على المشاركة في اتخاذ القرار					

محور استدامة ريادة الخدمات

م	العبارات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تعمل الهيئة على زرع ثقافة التميز في تقديم الخدمات لدي الموظفين					
2	تقوم الهيئة بتدريب الموظفين على أحدث الأساليب المستخدمة في تقديم الخدمات					
3	تقوم الهيئة بعمل استبيانات منتظمة للتعرف على اراء العملاء في الخدمات المقدمة					
4	تهتم الهيئة بتجديد خدماتها بصفة مستمرة ودورية					
5	تقوم الهيئة باستخدام الأساليب التكنولوجية الحديثة لزيادة مستوى جودة الخدمات					
6	تهتم الهيئة باستخدام أساليب التقييم التي تساهم في تحديد مستوى جودة الخدمات المقدمة للعملاء					
7	تهتم الهيئة بتقوية العلاقات مع الجهات المساعدة في تقديم الخدمة					

8	تقوم الهيئة بالعمل على حل كافة المشكلات التي تعيق تنفيذ الأهداف الاستراتيجية بكفاءة وفاعلية					
9	تعمل الهيئة على تكوين فرق العمل التي تساهم في زيادة جودة الخدمات المقدمة للعملاء					
10	تمنح الهيئة مكافآت وحوافز للموظفين المبدعين التي تقدم أفكار ابتكارية تساعد في تنمية وتطوير إجراءات ونظم العمل					
11	تهتم الهيئة بتحديث وتطوير أنظمة وإجراءات العمل					
12	تعمل الهيئة على اطلاع الموظفين بكل ما هو جديد في مجال تقديم الخدمات					
13	تعمل الهيئة على تشجيع الموظفين على اقتراح أفكار تساهم في تطوير نظم العمل					
14	تعمل الهيئة على توفير الدعم الكامل للموظفين لتوفير أفضل مستوى جودة حياة ممكن					
15	تعمل الهيئة على توفير المرونة التي تساهم في زيادة القدرة على مواكبة أي تغيرات يمكن ان تحدث في نظم العمل					

بحث بعنوان:

التهديدات السيبرانية الناشئة للخدمات الرقمية بالهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ وطرق التعامل معها

الباحث / عبد الرحيم علي محمد عبد الرحيم الانصاري
باحث أكاديمي
الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ

الملخص

تهدف هذه الدراسة إلى التعرف على أهم التهديدات السيبرانية التي قد تواجه الخدمات الحكومية الرقمية في الهيئة وطرق التعامل معها حيث أستخدم المنهج الوصفي، ويتضمن توصيف وتفصيل الطبيعة ونطاق هذه التهديدات بما في ذلك أنواع الاختراقات والهجمات المحتملة والأذى الذي يمكن أن يلحقها بالخدمات في الهيئة، ويهدف إلى إلقاء الضوء على المشاكل الحالية وتحديد النقاط الضعيفة في الأمان والموثوقية حيث أجري عدد من المقابلات مع خبراء الأمن السيبراني في الحكومة الاتحادية والاطلاع على المؤشرات والتقارير المحلية حول نتائج الأمن السيبراني للأعوام الأخيرة.

وأظهرت النتائج بأن أكثر التهديدات شيوعا في المنطقة هي عمليات الاختراق للمعلومات والقرصنة وحجب الخدمات عن المتعاملين كما ساهم تطور الذكاء الاصطناعي في زيادة تعقيد عمليات الهجوم السيبراني وصعوبة الكشف عنها ولمعالجة هذه التهديدات وطرق التعامل معها أوصت الدراسة بضرورة استخدام تقنيات الذكاء الاصطناعي ذاتها في الكشف المبكر عن عمليات قبل الهجوم وحجبها عن الخدمات الرقمية.

كما أوصت الدراسة ضرورة تعزيز البحث والابتكار في مجال الأمن السيبراني لضمان تطوير حلول وقائية متطورة تواكب التهديدات المستجدة، وأوصت لإنشاء مركز مراقبة تشغيلي متكامل للأمن السيبراني يراقب البنية التحتية للخدمات الرقمية الحيوية والاستجابة السريعة لحوادث الأمن السيبراني مع ضرورة الالتزام بتوفير التدريب المستمر للموظفين حول أحدث التهديدات وكيفية التعامل معها

- **أولاً- مقدمة:**

في ظل التقدم السريع للعالم الرقمي، أصبحت الخدمات الحكومية الرقمية لا غنى عنها في دولة الإمارات؛ حيث تشكل هذه الخدمات أداة رئيسية في تسهيل حياة المواطنين والمقيمين على أرضها وتتميز هذه الخدمات بالسهولة والفعّالية في إتاحة الوصول السريع للمعلومات الشخصية والحكومية على مدار الساعة، وهي بذلك تسهل التواصل والتفاعل بين المتعاملين والمؤسسات الحكومية وقد ساهمت هذه الخدمات في تصدر الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ لقائمة أكثر القطاعات المتميزة في تقديم وتوفير كافة الخدمات الرقمية للمواطنين والمقيمين على أرض الدولة، ومن دون الحاجة إلى زيارة مراكز الخدمة المنتشرة في إمارات الدولة؛ ما يعزز دور الهيئة في الإسهام في تحسين جودة الحياة للمجتمع ورفاهيته بالتحول التقني وبالتوافق مع استراتيجية برنامج الإمارات للخدمة الحكومية المتميزة ، وتوفر تطبيقات الهيئة الرقمية، ومنها على سبيل المثال رحلة مميزة لتجربة المستخدم بالتطبيقات الذكية حيث يمكن للأفراد الوصول إلى الخدمات الرقمية وإنجاز جميع معاملاتهم مع المرفقات بكل سهولة ويسر، دون الحاجة إلى التنقل الجغرافي من موقع المتعامل إلى مراكز الخدمة بالإضافة إلى ذلك، تعمل هذه الخدمات على تحسين كفاءة وجودة الإدارة بالهيئة عن طريق الحد والتقليل من الإجراءات الروتينية وتسريع وتيرة تداول واستخدام المعلومات بين فئات المجتمع المختلفة.

وبرغم ما تتيحه الخدمات الحكومية الرقمية من فرصٍ ومزايا هائلة، إلا أنها تواجه تحدياتٍ ومخاطر متنامية، تتمثل أساساً في التهديدات السيبرانية التي تزايدت بشكل ظاهر في السنوات الأخيرة وتشكل هذه التهديدات خطرًا كبيرا على سلامة المعلومات والخصوصية للمتعاملين والمؤسسات الحكومية، ومدى توافرها على مدار الساعة للمتعاملين من غير انقطاع أو توقف

ولذلك، تسعى هذه الدراسة إلى استقراء التهديدات السيبرانية التي تتعرض لها الخدمات الرقمية للهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، وبحث طرق التعامل معها بالإضافة إلى ذلك، ترمي هذه الدراسة إلى إجراء تقييم شامل لتأثير هذه التهديدات المحتملة على سير عمل الخدمات الرقمية في الهيئة ويتركز التقييم على تقدير المخاطر المالية والتشغيلية فضلاً عن تأثيرها في سمعة الدولة عامة والسمعة المؤسسية للهيئة خاصة كما سيتم استعراض وتحليل أفضل الممارسات والاستراتيجيات التي أثبتت فعاليتها

وجدارتها في مواجهة والتعامل مع هذه التهديدات من قبل السلطات الحكومية في الدولة ، ويهدف هذا الاستعراض والتحليل إلى استخلاص الدروس المستفادة وتطبيقها لتطوير منظومة عمل سيبرانية تحافظ على أمن الخدمات الحكومية الرقمية بالهيئة، وتضمن استدامتها في المستقبل، وتهدف إلى تعزيز الأمن والحماية في بيئة الخدمات الحكومية الرقمية، وضمان استمرارية تقديم الخدمات بشكل موثوق وفعال لتحقيق هذه الأهداف

- **ثانياً- مشكلة الدراسة:**

في عصرنا الحالي، تعتمد خدمات الهيئة بشكل متزايد على أنظمة الخدمات الرقمية لتحسين الكفاءة التشغيلية وتعزيز الشفافية وتحسين إمكانية الوصول للمواطنين والمقيمين على أرض الدولة، وعلى الرغم من ذلك تشكل التهديدات السيبرانية الناشئة خطرًا كبيرًا على موثوقية وأمن هذه الخدمات الحيوية عبر الفضاء الالكتروني، ومن هنا تتبلور مشكلة الدراسة في تفسير وتحليل واختبار الآثار المحتملة للتهديدات السيبرانية الناشئة على الأمان والموثوقية للخدمات الرقمية بالهيئة ، وتتلخص في كيفية وضع الاستراتيجيات والتدابير الوقائية التي يمكن عن طريقها التعامل الناجح مع التهديدات السيبرانية الناشئة في الخدمات الرقمية للهيئة، وكيف يمكن لبرامج التوعية السيبرانية للموظفين والعاملين في الهيئة في تحسين مستوى الأمن السيبراني للخدمات الرقمية واستدامة توفرها على مدار الساعة.

- **ثالثاً - تساؤلات الدراسة:**

وتتفرع عن المشكلة البحثية عدة تساؤلات، أهمها:

1. ما هي التهديدات السيبرانية الناشئة المحددة التي تشكل مخاطر على الخدمات الرقمية بالهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ؟
2. كيف هذه التهديدات على عمليات الهيئة، بما في ذلك المخاطر المالية والتشغيلية والسمعة المؤسسية؟
3. ما هي أهم الاستراتيجيات والتدابير الوقائية التي يمكن اتخاذها للتعامل الفعّال مع التهديدات السيبرانية في الخدمات الرقمية بالهيئة؟
4. كيف يمكن توفير التوعية السيبرانية المستمرة والتطوير المستمر للموظفين بالهيئة لتحسين مستوى الأمن السيبراني في الخدمات الرقمية؟

- **رابعاً - حدود الدراسة:**

سوف تتم معالجة هذه المشكلة البحثية، بالتركيز على حالةٍ دراسية واحدة وهي الهيئة

الاتحادية للهوية والجنسية والجمارك وأمن المنافذ وهذا هو النطاق المكاني للدراسة. وتركز هذه الدراسة على تحليل وتقييم التهديدات السيبرانية الناشئة وتأثيرها على الخدمات الرقمية للهيئة وعليه، فإنّ حدود التطبيق تتمثل فقط في التهديدات السيبرانية المتعلقة بالخدمات الرقمية.

- **خامساً - أهمية الدراسة:**

تنبع أهمية هذه الدراسة من ضرورة تعزيز مستوى الأمن السيبراني للخدمات الحكومية الرقمية في الهيئة لحمايتها من مخاطر التهديدات السيبرانية الناشئة حيث تهدف الدراسة إلى تحديد وتحليل أهم التهديدات مثل برامج الفدية والاحتيال التصيدي وهجمات اليوم الأول وهجمات حجب الخدمة وإلخ من التهديدات الشائعة كما تهدف إلى تقييم تأثير هذه التهديدات على عمليات الهيئة وخدماتها الرقمية، وتسعى الدراسة أيضًا لاستخلاص أفضل الممارسات والاستراتيجيات المستخدمة لمعالجة هذه التهديدات حيث ستتم دراسة الحالات الناجحة وتحليل الدروس المستفادة لتحديد أكثر المناهج فعالية لتعزيز الأمن السيبراني في الهيئة كما تهدف الدراسة إلى توفير الدعم التوعوي والتوجيهي للموظفين لتحسين منظومة الأمن السيبراني في الهيئة

- **سادساً - أهداف الدراسة :**

تتحدد أهداف هذه الدراسة فيما يلي:

1. تحديد أكثر التهديدات السيبرانية الناشئة التي تشكل خطراً على الخدمات الرقمية بالهيئة.
1. تقييم التأثير المحتمل لهذه التهديدات السيبرانية الناشئة على عمليات الهيئة وخدماتها الرقمية بما في ذلك المخاطر المالية والتشغيلية والمتعلقة بالسمعة المؤسسية.
1. تحديد وتوثيق أفضل الاستراتيجيات والتدابير الوقائية الناجحة التي يمكن اتخاذها للتعامل مع التهديدات السيبرانية الناشئة في الخدمات الرقمية بالهيئة.
1. توفير التوعية السيبرانية المستمرة والتطوير المستمر للموظفين بالهيئة لتحسين مستوى الأمن السيبراني في الخدمات الرقمية.

- **سابعاً - مراجعة الدراسات السابقة:**

سعت دراسة مي الخليفة (2023) إلى فهم مستوى تأثير التحول الرقمي في وزارة العدل بدولة قطر على أمن المعلومات فيها ومن أجل ذلك، اعتمدت الدراسة على

أدوات التحليل الوصفي والمسح الميداني لجمع البيانات، حيث تم استخدام استبانة لاستطلاع آراء عينة من العاملين والمسئولين في الوزارة وتوصلت الدراسة إلى أنّ هناك تأثير معنوي مهم للتحول الرقمي في الخدمات الحكومية على تحقيق الأمن السيبراني وبالإضافة أشارت الدراسة إلى أهمية التزام الجهات الحكومية بمعايير جودة الخدمات الرقمية وتوعية الجمهور بالخدمات الرقمية وأهميتها في تحقيق الأمن السيبراني وأوصت الدراسة بضرورة التركيز على حفظ الأمن المعلوماتي والمعلومات الحكومية الرقمية عن طريق تعزيز الوعي بأهمية الأمن السيبراني وتوفير المرافق الأساسية للتحول الرقمي كما أوصت بضرورة وجود وحدات تنظيمية متخصصة في أمن المعلومات وتكنولوجيا المعلومات في المؤسسات الحكومية وبالرغم استفادة الباحث من التحديات المرتبطة بالأمن السيبراني فإن تكنولوجيا المعلومات والاتصالات لا تزال تمثل فرصة كبيرة لتحقيق تنمية مستدامة وخدمة للمجتمعات البشرية حيث تتركز دراستنا على تسليط الضوء على التحديات الأمنية المتعلقة بتكنولوجيا المعلومات والفضاء السيبراني مما يتطلب الأمر المزيد من الاهتمام والمجهود المضاعف باستمرار لحماية البيانات والمعلومات الحكومية من هجمات القرصنة والتجسس والاختراقات السيبرانية والالتزام بتوفير التدريب والتوعية للموظفين بشأن مخاطر الأمن السيبراني وكيفية التصدي لها.

تناولت دراسة طوابير عبدالجليل إلى فهم استراتيجيات الأمن السيبراني في ضوء التهديدات المتزايدة التي تواجه الأفراد والمنظمات والدول في العصر الرقمي، وتركز الدراسة على تجربة دولة الإمارات العربية المتحدة في هذا المجال، حيث أولت الإمارات اهتمامًا كبيرًا للأمن السيبراني، ومنحته أولوية قصوى، واعتمدتها كحالة دراسية يتم فيها فهم الحالة بعمق ودراسة تأثيراتها وعملياتها والعوامل المؤثرة فيها، وتوصلت أبرز النتائج الاختراقات والهجمات السيبرانية ستكون في المستقبل أكبر وأكثر كلفة ولها تأثير قوي على البنية التحتية للدولة وبالتزامن مع الانتشار السريع للأجهزة الذكية ونمو الشبكة العنكبوتية وتزايد المدن الذكية وتطبيقاتها المتنوعة ، وختمت الدراسة بتوصياتها بضرورة تطبيق منظومة الدفاع السيبراني في القطاعات الحيوية وتفعيل منظومات الحماية وسياسات الأمن السيبراني وتكثيف الوعي بين المنظمات، على الرغم من ذكر الدراسة أن الحالة الدراسية لدولة الإمارات العربية المتحدة إلا أنه لم تُقَارَن حالة الإمارات بدول أخرى متقدمة في مجال الأمن السيبراني، مما يضعف قيمة النتائج علما تركز دراستنا على أهمية فهم ودراسة التهديدات السيبرانية وتحديدها وأثرها على الخدمات الحكومية الرقمية بالهيئة، وفي دولة الإمارات بالتحديد مع الاطلاع على أفضل الممارسات في

مجال الأمن السيبراني للدول المتقدمة والمتصدرة للتصنيف العالمي.

تناولت دراسة زمورة جمال وبن عيسى ليلى عن تحول الجزائر إلى الحكومة الإلكترونية والتحول الرقمي للخدمات العمومية؛ مما استدعى الاهتمام بالأمن السيبراني، والذي يشكل الهاجس الأكبر للدول وخاصة مع الانفتاح الكلي على الفضاء السيبراني وتحدياته حيث أُعْتُمِد منهج وصفي تحليلي في هذه الدراسة، وجُمِعَت المعلومات والبيانات ذات الصلة بالأمن السيبراني وتحليلها بشكل تفصيلي وأيضا مراجعة الأدبيات العلمية والمصادر الموثوقة لاستخلاص المعلومات المتعلقة بالتهديدات السيبرانية مع زيادة التهديدات والمخاطر، وتشير النتائج إلى وجود نقائص واختلالات ملحوظة في الإجراءات التنظيمية والجوانب التقنية في الجزائر مقارنةً بالمعايير الدولية وختمت الدراسة بتوصياتها الاستفادة من تجارب الدول الرائدة في مجال الأمن السيبراني إقليميا ودوليا سواء عن طريق الاتفاقيات الثنائية لتبادل الخبرات والانضمام إلى المنظمات في مجال حماية أنظمة المعلومات والأمن السيبراني ، وعلى الرغم من أن الدراسة على الاتفاقيات بين الدول في مجال الأمن السيبراني والمتعارف عليه أنه ربما لا تكون هناك التزام وتطبيق على بنودها في أرض الواقع ولا يوجد رقابة على تنفيذها ومخرجاتها في تقليل التأثيرات على الأمن السيبراني إلا أن دراستنا تتناول على العكس تعمقًا أكثر في تبني أفضل الممارسات المطبقة والعملية التي تخدم شريحة واسعة من المجتمع في مجال الأمن السيبراني وتحسين الإجراءات التنظيمية الإدارية والجوانب التقنية المتعلقة بالأمن السيبراني في الخدمات الرقمية للهيئة

تناولت دراسة روس اندرسون، عن الهندسة الأمنية كدراسة سابقة متعددة الجوانب والمجالات تتضمن الدراسة تحليلاً شاملاً للتهديدات والمخاطر التي تواجه الأنظمة والشبكات الحاسوبية وتحديد الضعف في التصميم والتهديدات الأمنية المحتملة وتأثيراتها المحتملة على النظام، زيادة على ذلك تركز الدراسة على تطوير وتحسين تقنيات وأدوات تصميم الأمان مثل استخدام التشفير وتطبيق بروتوكولات الأمان وتطوير سياسات الأمان لحماية الأنظمة والبيانات كما تشمل الدراسة أيضًا أساليب وأدوات لاختبار أمان الأنظمة والتحقق منها، ويستخدم المنهج العلمي في تقديم المفاهيم والمعلومات المتعلقة بالهندسة الأمنية حيث يعتمد الكاتب على جمع المعلومات من مصادر موثوقة وتحليلها وتقييمها باستخدام المفاهيم والنظريات العلمية، ويقدم الكتاب مبادئ وتقنيات لتصميم وتنفيذ الأنظمة الموزعة الموثوقة، ويشجع على إجراء التحقق والتقييم المستمر للأنظمة المصممة، وتشير النتائج إلى أهمية بناء فهم شامل للأمان والتهديدات والتحديات التي تواجه

الأنظمة الموزعة حيث يقدم المفاهيم والنظريات اللازمة لفهم جوانب الأمان والتصميم الآمن، ويساهم الكاتب في زيادة الوعي الأمني لدى المهندسين والمطورين وأصحاب القرار في مجال الأمان يساعد على فهم أهمية تكامل الأمان في جميع مراحل تطوير الأنظمة المختلفة، وختمت الدراسة بتوصياتها لتشجع على استخدام أفضل الممارسات في مجال الأمان وتنفيذها في تصميم وتطوير الأنظمة الموزعة يتضمن ذلك استخدام تقنيات التشفير الآمنة وتطبيق السياسات الأمنية القوية ، على الرغم أن الدراسة ترتكز على تحليل التهديدات والمخاطر التي تواجه الأنظمة والشبكات الحاسوبية إلا أنه يتضح عدم كفايته في تمثيله لمجتمع الهندسة الأمنية كتمثيل عيني والتي يجب ان تكون شاملة لشريحة معينة للمجتمع مماقد يقلل من من قدرة الدراسة على تعميم النتائج وفي الجانب الاخر ترتكز دراستنا على دراسة توفير أفضل الممارسات السيبرانية في تطوير انظمة الدفاع الخاصة في الخدمات الرقمية لفئة المواطنين والمقيمين على ارض الدولة .

تناولت دراسة تشين زي، هان لي، شونغشو يو ، التركيز على دور الحوكمة الرقمية وخدمات الحكومة الإلكترونية في تعزيز النمو الاقتصادي وتحسينها في الصين حيث تم استخدام منهجية تقنية تعتمد على «esnefeD tegraT gnivoM»(DTM) وهي تقنية بمثابة استراتيجية ديناميكية للأمن السيبراني تهدف إلى حماية أنظمة الكمبيوتر والشبكات والبيانات بشكل استباقي

وتم اقتراح النموذج الجديد لنظام دخول الوصول الديناميكي لتطبيقات الويب ويهدف هذا النموذج إلى تحويل الكلمات الثابتة في عناوين إلى كلمات ديناميكية وعشوائية مما يزيد بشكل كبير من تكلفة الهجمات السيبرانية ويضعفها حيث تم تقييم النموذج من خلال معيار الكفاءة والفعالية عن طريق تجربة عملية أظهرت النتائج التجريبية أن النموذج عملي وفعال في تحقيق أهدافه وعلى الرغم من النتائج الإيجابية لا أنه يجب أن يقدم المزيد من التحليل والتقييم للنموذج بما في ذلك تقييم تأثيره على أداء تطبيقات الحكومة الإلكترونية الفعلية ومدى تكاملها مع البنية الإلكترونية القائمة عليها علما ترتكز دراستنا على إسقاط الضوء على أبرز التهديدات السيبرانية على الخدمات الرقمية جميعها سواء كانت تطبيقات الويب أو الهواتف المتحركة والأنظمة المكتبية وطرق التعامل معها والتي تشكل معضلة لاستمرارها في تقديم الخدمات الرقمية للمتعاملين عند وجود هجوم سيراني أثناء تشغيلها

تناول إنسان أنوري دراسته حول تقييم دور الإدارة العامة في مكافحة جرائم الإنترنت في إندونيسيا من خلال تحليل الأطر القانونية القائمة حيث تستخدم الدراسة المنهج البحثي

النوعي لتحقيق هدف الدراسة من خلال جمع البيانات من مصادر أولية مثل الوثائق القانونية والتشريعات والقوانين والأحكام القضائية، ومن مصادر ثانوية مثل المنشورات والمقالات حيث توصلت الدراسة إلى أن إندونيسيا لديها سياسات ومواد وأطر قانونية شاملة لفحص ومراقبة انتهاكات الأمن السيبراني ومكافحة جرائم الإنترنت ومع ذلك، فإن تنفيذ القوانين المصوغة بشأن الأمن السيبراني ومكافحة جرائم الإنترنت غير كافٍية وتشدد الدراسة على ضرورة أن تقوم الحكومة الإندونيسية بصورة فعالة بصياغة سياسات فعالة للأمن السيبراني، وتحديد خطوات شاملة للدفاع عن الهجمات السيبرانية، وتطوير سيادة القانون اللازمة لممارسة السيطرة السليمة على الهجمات السيبرانية في البلاد. على الرغم استخدام الدراسة للمصادر الأولية والثانوية من القوانين إلا أنه لم يُتَطَرَّق إلى حجم العينة من الإجمالي الوثائق القانونية وبالإضافة رُكِّز على السياسات والأطر القانونية، ولم يُقَدَّم تقييم شامل لفاعلية هذه السياسات والأطر القانونية وتأثيرها الفعلي على مكافحة جرائم الإنترنت وأثرها على الأمن السيبراني في بلد الدراسة حيث دراستنا الحالية ستحلل العوامل التي تؤثر في تنفيذ القوانين والسياسات للأمن السيبراني لغرض تحسين فعالية التنفيذ وتعزيز الأمن السيبراني في الهيئة

طرح خالد محمود مهران دراسته حول ضرورة تبني الدول لنظام التحول الرقمي وتطبيقه على مرافقها العامة والاستراتيجية والجهات العسكرية، وذلك لحماية أنظمتها الإلكترونية وفضائها السيبراني، وتتضمن الإجراءات التقنية إقامة جدران حماية، ونظم كشف التسلل، وتحسين أمان نظام أسماء النطاقات، وتعزيز البنى التحتية الحساسة، وتشفير الشبكات وعند عدم اتخاذ الدول الإجراءات الكافية لتأمين الفضاء الإلكتروني، فقد تتعرض لأضرار جسيمة لخدماتها

استخدام الباحث في الدراسة على المنهج التحليلي والذي يعتمد على مجموعة من التشريعات القانونية والمقالات المتخصصة والأبحاث والتجارب في هذا المجال حيث توصلت الدراسة على وجوب وضع استراتيجية وطنية للأمن السيبراني، وتشمل تحديث التشريعات السيبرانية وتنسيق التشريعات بين الدول وإنشاء وحدات متخصصة لتطبيق القانون وتعزيز الإجراءات الاستباقية والتوعية والتدريب

على الرغم من اعتماد الدراسة على الأساليب الفنية في دعم الفضاء السيبراني بأنظمة الحماية لشبكاتها وخدماتها إلا أنه لم يُسْتَعْرَض نقاط القوة والضعف والفجوات السيبرانية الواجب اتخاذ التدابير اللازمة في التقليل من تأثيرها في حالة تعرضها للخطر إلا أن دراستنا ترتكز على تحديد أبرز التهديدات السيبرانية المهددة لبقاء الخدمات الرقمية في الفضاء

السيبراني للهيئة العمل واستمرارية تقديم الخدمات للمتعاملين.

طرحت اللجنة الاقتصادية والاجتماعية لغربي آسيا في منظمة الأمم المتحدة دراستها حول الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية على تحديد وتحليل التهديدات السيبرانية التي تواجهها المؤسسات والأفراد في المنطقة حيث حُلِّل أنواع الهجمات السيبرانية المنتشرة، مثل هجمات الاختراق، والتصيّد الاحتيالي (gnihsihP)، والبرمجيات الخبيثة (erawlaM)، والهجمات المنسقة لنفي الخدمة (SoDD) وأُسْتُعْرِضَت الثغرات الأمنية الشائعة في البنية التحتية الحيوية والأنظمة الحكومية، بما في ذلك ضعف التكوين الأمني، وقصور في التحديثات الأمنية، وسوء الإدارة الأمنية، وأظهرت الدراسة أن هناك تهديدات سيبرانية متزايدة في المنطقة العربية، وهي تهديدات تشكل تحديًا كبيرًا على الأمن السيبراني والاستقرار الاقتصادي والسياسي، وأن الجهات المهاجمة تستفيد من التقنيات المتقدمة والأدوات المتطورة لتنفيذ هجماتها، وتستهدف على نحو خاص المؤسسات الحيوية والبنية التحتية الحكومية وأبرز التوصيات التي توصلت إليها تحسين الأمان السيبراني وتعزيز قدرة المنطقة العربية على مكافحة الجرائم السيبرانية من خلال تحسين التشريعات السيبرانية وتعزيز القدرات القانونية لمكافحة الجرائم السيبرانية وزيادة التعاون الدولي والمحلي والقطاعي لتعزيز قدرات الدفاع والاستشارة والتوعية السيبرانية

على الرغم من تركيز الدراسة على الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية إلا أنه لوحظ وجود تحديات في الحصول على بيانات شاملة ومحدثة حول أكثر التهديدات السيبرانية في المنطقة العربية بسبب حساسية هذه المعلومات وتركيزها في الدوائر الأمنية والحكومية في البلاد العربية الا ان دراستنا ستقوم في دراسة وتحليل البيانات المتاحة وفهم التحديات السيبرانية في الهيئة وتفاصيل هذه الهجمات

هدفت دراسة شيفتشينكو والآخرون على فهم طبيعة الخسائر الناجمة عن الأحداث المتعلقة بالسيبرانية عبر فئات المخاطر المختلفة وقطاعاتها كما هدفت الدراسة إلى تحليل توزيع التكرار وشدة الخسائر المتعلقة بتلك الأحداث وفقًا لفئات المخاطر وقطاعات الأعمال وأظهرت الدراسة أن تكرار الأحداث المتعلقة بالسيبرانية قد زاد بشكل كبير بين عامي 8002- 6102 كما تبين أن تكرار وشدة الخسائر وتعتمد على قطاع الأعمال ونوع التهديد السيبراني وأظهرت الفئات الأكثر أهمية من حيث عدد الأحداث هي اختراقات البيانات وكشف البيانات غير المصرح بها، بينما أظهرت الممارسات السيبرانية الأخرى مثل

الابتزاز السيبراني والتصيّد والتزييف كما توصلت الدراسة بأنه يجب وضع استراتيجيات إدارة المخاطر المناسبة ودعم الاستثمار في التخفيف الأمثل من المخاطر بناءً على فهم أفضل للأحداث المتعلقة بالسيبرانية لفئات المخاطر المختلفة وقطاعات الأعمال.

على الرغم من إظهار الدراسة تكرار الأحداث السيبرانية بين أعوام محددة الا أنه لوحظ إلى أن قلة البيانات التاريخية حول الخسائر الناجمة عن المخاطر السيبرانية والتي قد تعد تحديًا لتحليل تكرار وشدة الأحداث المتعلقة بالسيبرانية في المستقبل الا أنه دراستنا ترتكز على دراسة وفهم الوثائق والتقارير الفنية التعقيبيه على الاحداث السيبرانية في الهيئة بحيث يتم التركيز على طبيعة ونمطية التهديدات ومدى تكرارها بالمستقبل

ترتكز دراسة إريكا دي لونيرجان ، جاكلين شنايدر على تحليل وتقييم التهديدات التي يواجهها النظام السيبراني للحكومة الأمريكية ويتم تسليط الضوء على الهجمات السيبرانية الحديثة والمتقدمة التي تستهدف البنية التحتية الحكومية والبيانات الحساسة وسلطت الضوء على استراتيجيات الدفاع السيبراني التي اتبعتها وزارة الدفاع الأمريكية في السنوات السابقة لهدف تحليل فعالية هذه الاستراتيجيات وتحديد النقاط الضعيفة والتحديات التي تواجهها وتوصي الدراسة بضرورة تحديد معايير سلوك واضحة في مجال السيبرانية وتعزيز قدرة الحكومة على استخدام أحدث التقنيات والحلول الأمنية وأيضًا الاستثمار في تدريب الكوادر البشرية وزيادة الوعي حول التهديدات السيبرانية والإجراءات الوقائية اللازمة وتعزيز التعاون بين القطاعين العام والخاص في مجال السيبرانية، وتبادل المعلومات والخبرات لمواجهة التهديدات السيبرانية المتطورة

على الرغم من تركيز الدراسة على دراسة الاستراتيجية الدفاعية في الامن السيبراني الا انه قد يظهر تحيز في التحليل والتقييم هذه الاستراتيجيات والتوصيات بسبب وجهات نظر وخلفيات الباحثين المشاركين في الدراسة الا أننا سنقوم بإجراء مقابلات مع جهات اتحادية في مجال الامن السيبراني لفهم طبيعة ومصادر والدفاعات السيبرانية الناجعة للتأكد من فاعليتها على خدمات وانظمة الهيئة الرقمية

والخلاصة أنّ معظم الدراسات السابقة توصلت إلى أن الخدمات الحكومية الرقمية تتعرض لمجموعة واسعة من التهديدات التي تشمل الاختراقات السيبرانية، والهجمات الضارة المستهدفة، وسرقة المعلومات، وتعطيل الخدمات، والتلاعب بالبيانات. وقد تسبب هذه التهديدات في تأثيرات خطيرة مثل فقدان البيانات الحساسة، وتعطيل الخدمات الرقمية، والتأثير على الثقة العامة في خدمات الهيئة والتعامل معها. وقد عرضت هذه الأدبيات بعض الاساليب الرئيسية لمكافحة هذه التهديدات، واهمها تعزيز

الوعي السيبراني والتدريب للموظفين والعاملين في الهيئة، وتنفيذ إجراءات الأمان القوية، وتطوير القدرات التقنية اللازمة للكشف المبكر والاستجابة الفعالة للهجمات السيبرانية على مدار الساعة

كما تشير الدراسات السابقة إلى أهمية تعزيز التعاون والتنسيق بين جميع اصحاب المصلحة في مجال الأمن السيبراني لتبادل الخبرات والممارسات وتعزيز التشريعات والسياسات السيبرانية لحماية البنية التحتية الرقمية وبالإضافة إلى ذلك يتم التركيز على أهمية التطوير والتوعية ويتطلب التطوير الاستمرار في تحسين التقنيات والأدوات الأمنية، وتحديث البرامج والنظم بانتظام ومراجعة السياسات والإجراءات لمواكبة التهديدات الجديدة مع توفير تدريبات منتظمة وحملات توعية لتعزيز الممارسات الأمنية والتصدي للهجمات السيبرانية. وبشكل عام، تعكس مراجعة الدراسات السابقة أهمية مكافحة التهديدات السيبرانية المستهدفة للخدمات الرقمية، وتوفر إطارًا ملائماً للتحليل في هذا المجال. ومن هنا، تنبع أهمية هذه الدراسة؛ حيث تركز على إلى تعزيز مستوى الامن السيبراني للخدمات الحكومية الرقمية في الهيئة من التهديدات السيبرانية الناشئة ويتضمن البحث تحديد وتحليل التهديدات مثل برامج الفدية والاحتيال التصيدي وهجمات اليوم الأول وهجمات حجب الخدمة ويهدف البحث أيضًا إلى تقييم التأثير المحتمل لهذه التهديدات على عمليات الهيئة وخدماتها الرقمية وتحديد المخاطر المالية والتشغيلية والمتعلقة بالسمعة بالمؤسسية بالإضافة يهدف البحث إلى استخلاص أفضل الممارسات والاستراتيجيات المستخدمة بنجاح من قبل السلطات الحكومية في الدولة لمعالجة هذه التهديدات وستتم دراسة الحالات وتحليل الدروس المستفادة لتحديد المناهج الفعالة التي يمكن تبنيها لتعزيز الأمن السيبراني للخدمات الحكومية في الهيئة وضمان استمرارية خدماتها الرقمية مع توفير الدعم التوعي والتوجيهي للموظفين لتحسين منظومة الامن السيبراني في الهيئة

- **ثامناً - منهج البحث:**

أنواع مصادر البيانات المستخدمة في الدراسة:

يستقي الباحث مصادره من مصادر أولية وأخرى ثانوية وتتمثل المصادر الأولية أساسا في الوثائق الداخلية داخل الهيئة، مثل سياسات الأمن السيبراني وتقارير الحوادث وتقييمات الضعف، بالإضافة إلى تقارير وكالات الأمن السيبراني الحكومية كمجلس الامن السيبراني. أمّا المصادر الثانوية، فتتمثل في المصادر المكتبية والالكترونية، مثل الكتب والدوريات المتخصصة، ومواقع الانترنت الرسمية، بالإضافة إلى رسائل الماجستير والدكتوراة

التحليل الوصفي:

من أجل معالجة مشكلة الدراسة، من الضروري أن نُجري تحليلاً وصفياً للتهديدات السيبرانية الناشئة وتأثيراتها على الخدمات الرقمية بالهيئة ويتضمن التحليل الوصفي توصيف وتفصيل الطبيعة ونطاق هذه التهديدات بما في ذلك أنواع الاختراقات والهجمات المحتملة والأذى الذي يمكن أن يلحقها بالخدمات في الهيئة ويهدف هذا التحليل الوصفي إلى إلقاء الضوء على المشاكل الحالية وتحديد النقاط الضعيفة في الأمان والموثوقية حيث يساعد على فهم الظواهر والمتغيرات المختلفة وتصنيفها وتوصيفها بشكل دقيق بالإضافة فإن الاستدلال السببي يعتمد على الوصف المتأني ويمكن استخدام البيانات الوصفية لتحليل العلاقات السببية بين المتغيرات وتفسير النتائج التي تم الحصول عليها باختصار يعمل التحليل الوصفي على توضيح الحالة الحالية وفهم الظواهر المرتبطة بالتهديدات السيبرانية الناشئة بينما يساهم الاستدلال السببي في فهم العلاقات والتأثيرات المحتملة بين متغيرات الدراسة عليه.

دراسة الحالة:

يُعد أسلوب دراسة الحالة أحد الأدوات المنهجية المهمة، وفيه يتم جمع أكبر قدر ممكن من المعلومات عن الحالة محل الدراسة، وهي الخدمات الرقمية بالهيئة ومحاولة معالجة مشكلة الدراسة في كيف يمكن تحسين مستوى الامان والموثوقية للخدمات الرقمية بالهيئة والتقليل من تأثيرات التهديدات السيبرانية وتستهدف دراسة الحالة دراسة اكثر التهديدات الشائعة على الخدمات الرقمية وتكون دراسة هذه الحالة بشكل مستفيض يتناول كافة المتغيرات المرتبطة بها، وتناولها بالوصف الكامل والتحليل ويمكن أن تستخدم دراسة الحالة كوسيلة لجمع البيانات والمعلومات في دراسة وصفية، وكذلك يمكن تعميم نتائجها على الحالات المشابهة، بشرط أن تكون الحالة ممثلة للمجتمع الذي يُراد الحكم عليه ويوظف الباحث أداة دراسة الحالة الداخلية الطولي (esac-nihtiw lanidutignol sisylana)، التي تسمح بتحليل واستقراء حالةٍ دراسية واحدة خلال فترة زمنية محددة.

المقابلات:

تم إجراء مقابلات مع خبراء الأمن السيبراني وأفراد من ذوي الخبرة لجمع المعلومات والتوصل إلى رؤى قيمة حول التهديدات السيبرانية والتحديات المشابهة عند تنفيذ هذه الخطوات بشكل متقن ومنهجي، ستساعد المنهجية في تحقيق أهداف البحث وتوفير رؤى قيمة في مجال الأمن السيبراني.

الملاحظة:

تم توظيف هذه الأداة المنهاجية المهمة في جمع البيانات الخاصة بهذه الدراسة، ومعالجة مشكلتها البحثية، والإجابة عن بعض تساؤلاتها؛ كون الباحث يعمل بالهيئة الاتحادية للهوية والجنسية والجمارك وامن المنافذ منذ عام 2002 في قسم تقنية المعلومات ولديه من الخبرات الكبيرة في مجال الامن السيبراني وامن الخدمات العمليات.

الفصل الثاني

التهديدات السيبرانية الناشئة على الخدمات الرقمية بالهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ: تحليل وتقييم المخاطر

يتضمن هذا الفصل مبحثين حيث يعمد المبحث الأول إلى دراسة حالة التهديدات السيبرانية الناشئة المحددة التي تشكل مخاطر على الخدمات الرقمية للهيئة الاتحادية للهوية والجنسية والجمارك وامن المنافذ فيما يختبر المبحث الثاني التأثير المحتمل للتهديدات السيبرانية الناشئة على العمليات الرقمية بالهيئة.

المبحث الأول

- **التهديدات السيبرانية الناشئة المحددة**

الرقمنة هو مفهوم لتعزيز وتطور الخدمات الحكومية من خلال تحويل العمليات التقليدية إلى صيغ رقمية وإلكترونية وتوفر الرقمنة خدمات حكومية مبسطة ومتاحة عبر الإنترنت مثل تجديد الاقامة واصدار التأشيرة ويسهل النظام الرقمي الوصول إلى الخدمات ويقلل البيروقراطية وتعزز الرقمنة شفافية الحكومة والتحول الرقمي في الخدمات الحكومية ويسهم في تحسين الكفاءة والشفافية وتعزيز التواصل بين الحكومة والمواطنين، ويعزز التنمية المستدامة وتعد الخدمات الرقمية الحكومية من أهم الوسائل التي تسهم في تطوير العمل الحكومي وتحسين جودة الخدمات المقدمة للمواطنين والمقيمين في الدولة، وفي ظل تطور التكنولوجيا وتطور الاتصالات، أصبحت هذه الخدمات متاحة عبر الإنترنت وتعتمد بشكل كبير على البنية التحتية الرقمية ومع ذلك، فإن هذا التطور التكنولوجي يفتح الباب أمام تهديدات جديدة، وأحد هذه التهديدات هو التهديد السيبراني ويشير مفهوم الأمن السيبراني في الخدمات الرقمية إلى الإجراءات والسياسات التي تتخذها الحكومات لحماية البيانات والمعلومات الحساسة التي تتعامل معها ويهدف الأمن السيبراني إلى حماية هذه البيانات من الوصول غير المصرح به، والتسبب في تلف أو تعديل البيانات دون إذن مسبق والتلاعب بالخدمات الرقمية لتعطيلها أو تقويض كفاءتها

مما يفترض من القائمين في مهام الأمن السيبراني في الخدمات الرقمية الحكومية تنفيذ إجراءات وسياسات فعالة للحماية من الهجمات .

وتمثل التهديدات السيبرانية بشكل عام التحديات والمخاطر التي تنشأ من استخدام التكنولوجيا الرقمية، وتشمل الهجمات الإلكترونية والاختراقات الهجومية وسرقة المعلومات وتعد هذه التهديدات أمرًا ذا أهمية كبيرة حيث تؤثر على الأمن الاقتصادي والسياسي وتهدد خصوصية الأفراد والمؤسسات والحكومات في العالم، وتعد دولة الامارات من الدول الرائدة في تقديم الخدمات الحكومية عبر المنصات والانظمة الذكية والخدمات الرقمية ونظرا لتسارع وتيرة انتقال الخدمات الى النطاق الرقمي وعبورها الى انظمة السحب الرقمية تزداد على اثرها المخاطر السيبرانية وتتعدد الاختراقات الهجومية وتسهل سرقة المعلومات وتعطيل الأنظمة الحاسوبية والتلاعب بالبيانات و الوصول غير المشروع إلى المعلومات الحساسة وتكويـــن فوائد غير قانونية ، والتسبب لأضرار للأفراد والمؤسسات والحكومات علما حيث كلما زاد اتساع حجم وعدد الخدمات الرقمية بالأمارات زادت على اثرها تعرضها للهجمات الرقمية عليها بمعدلات كبيرة قد تصل إلى (200) الف محاولة لهجمة سيبرانية في اليوم الواحد مما يعزز اهمية وموقع الامن السيبراني في الخدمات الرقمية بالدولة وقد احتلت دولة الامارات مرتبة متقدمة في مجال الامن السيبراني بين دول العالم قبل اعوام مضت وبسبب اهتمام القيادة الرشيدة في اعطاء الامن السيبراني الدعم اللازم بالتشريعات والقوانين والانظمة التقنية وخطة الدولة في التحول الرقمي ارتفعت مرتبة الامارات لتصل الى مراتب متقدمة على مستوى العالم في مجال الامن السيبراني بسب تظافر جميع الجهود بين قطاعات الدولة.

ومن خلال مشاركتي في مؤتمر الامن في القطاع العام بالأمارات، لاحظت طرح مؤشرات يستدل منها في زيادة بالهجمات السيبرانية على الحكومات بشكل ملحوظ في السنوات الاخيرة ، مما شكل تحديا وتهديدًا حقيقيًا للأمن القومي وأظهرت التقارير المنشورة بالمؤتمر أن هذه الهجمات أصبحت أكثر انتشارًا وتعقيدًا وتنوعًا من السابق ، مما تطلب تعزيز الجهود لحماية البيانات والأنظمة الحكومية وتشير نتائج التقرير ايضا إلى أن الهجمات السيبرانية على الحكومات تهدف خصوصا إلى سرقة المعلومات الحساسة، وتعطيل الأنظمة الحيوية، والتأثير على العمليات الحكومية الرقمية.

ويعد التطور السريع هو أحد أهم خصائص التي تسرع التهديدات السيبرانية الناشئة، حيث كشف تقرير منظمة الأمن والتعاون في أوروبا لعام 2021 أن 09% من التهديدات الجديدة المكتشفة خلال العام كانت قادرة على التطور لتفادي تقنيات الكشف والمواجهة

خلال فترة زمنية قصيرة بين 3 إلى 12 شهرا ويعزى هذا التطور السريع إلى استغلال المهاجمين لتقدم التقنيات الموجودة.

وتتنوع أساليب الهجوم المستخدمة ضد بنية تكنولوجيا المعلومات بشكل كبير، حيث تشمل تقنيات حديثة مثل البرمجيات الضارة والذكاء الاصطناعي، بالإضافة إلى الطرق التقليدية المعروفة وقد أشار تقرير مكتب مكافحة الجريمة الإلكترونية لعام 2012 إلى وجود أكثر من 500 طريقة للهجوم تراوحت بين البسيطة والمتقدمة ، ومن خلال إتاحة أدوات القرصنة والهجوم السيبراني بكل حرية على الإنترنت وبتكلفة بسيطة ومجانية وتسهم بشكل قوي في انتشار تلك التهديدات وأظهر تقرير لمنظمة لوكالة الاتحاد الأوروبي للأمن السيبراني (ASINE) أن نسبة كبيرة من برمجيات القرصنة المستخدمة كانت متاحة للجميع دون أي مقابل مثل توفير خدمات «استئجار المهاجمين» عبر الإنترنت بشكل موسع خارج نطاق الانظمة والقوانين في حكومات العالم .

وتشير الأبحاث إلى ظهور أنماط جديدة ومتخصصة من البرمجيات الضارة تستهدف قطاعات ومؤسسات معينة بدقة أكبر حيث تم تصنيف فئة من فيروسات الفدية (erawmosnaR) لغرض استهداف المنشآت الصحية وقطاع الرعاية الصحية، بالإضافة إلى البنوك والمؤسسات المالية، وقد تبين أن هذه البرمجيات الضارة تعتمد على تقنيات الذكاء الاصطناعي والتعلم الآلي في تحليل خصائص المستهدف وسلوك مستخدميه لزيادة كفاءة عمليات الهجوم كما تستخدم تقنيات التخفي والتزوير لتفادي برمجيات الكشف والحماية المستخدمة لصد عن محاولة الهجوم.

وشهدت عمليات الاحتيال عبر شبكة الإنترنت تطوراً ملحوظاً خلال السنوات الأخيرة من خلال استخدام تقنيات متقدمة للتضليل وخداع الضحايا مثل عمليات التلاعب بالمحتوى السمعي البصري (ekaf peeD) التي تستند إلى تقنيات الواقع الافتراضي والذكاء الاصطناعي لتزوير الوسائط الرقمية بشكل موثوق، وايضا تطورت عمليات سرقة هويات المستخدمين من خلال استخدام نماذج التعلم العميق والتعلم الآلي في تحليل بيانات مواقع التواصل الاجتماعي لاستنباط المعلومات الشخصية لضحايا الاحتيال.

تم ملاحظة انه ساهم التطور التقني السريع في نشوء أنماط منتشرة بشكل واسع من التهديدات السيبرانية، حيث تتيح تقنيات مثل الحوسبة السحابية وخدمات الإنترنت الأمر (Saal ecivreS-a-sa-tenretnI) للمهاجمين السيبرانيين والقراصنة من استغلال البنية التحتية لشبكات المعلومات وقواعد البيانات دون الحاجة للبنية التقنية المادية حيث يتيح هذا النموذج من تقديم الخدمات عبر الإنترنت في الوصول إلى موارد حاسوبية هائلة من

خلال عقود استئجار الخدمات وبأسعار منخفضة .

في مايو 2021 ، تعرضت بعض المؤسسات الحكومية والشركات الإماراتية لهجوم سيبراني متطور استهدف قواعد بياناتها، حيث تمكن المهاجمون من الولوج غير المصرح به عبر اللجوء الى حملة بريد إلكتروني مسعورة احتوت على برامج تجسسيه، ما أسفر عن سرقة معلومات شخصية ومالية لما يزيد عن 5 ملايين مستخدم وتمكنت الجهات الأمنية من تحديد مصدر الهجوم عبر تتبع عنوان بروتوكول الإنترنت المستخدم ،وأشار التحليل إلى أن الهجوم أطلق من خادم مصدره خارج الدولة ، كما تم استخدام تقنيات متقدمة للتهرب من الكشف وقد أدى الهجوم إلى الاهتمام الواسع في تشديد قوي لإجراءات الأمن السيبراني في القطاعين العام والخاص بالدولة ، وتم وضع خطة وطنية طويلة الأمد لتعزيز الأمن وحماية البنية التحتية لتقنية المعلومات في الدولة

ويعد دور مراكز مكافحة الجرائم الالكترونية في دولة الإمارات في مجال حماية البنية التحتية لتقنية المعلومات والاتصالات من التهديدات السيبرانية بالدور المحوري والمهم حيث تقوم هذه المراكز بمهمة الكشف والرصد المبكر عن أي محاولة للهجمات أو تهديدات سيبرانية عبر مراقبة حركة المعلومات والبيانات على الشبكات الحكومية والخاصة وباستخدام تقنيات كشف متطورة ، كما تقوم بتحليل بيانات التهديدات وتقديم الاستشارات الفنية لتعزيز القدرات الأمنية وتعمل المراكز على تنفيذ برامج التوعية الأمنية وتدعم الجهود الوطنية في مكافحة الجريمة الإلكترونية من خلال التعاون مع الجهات ذات العلاقة والمهمة بالدولة

خلال شهر ديسمبر من عام 2020 ، كشف التقرير الأمني الشهري لدولة الإمارات العربية المتحدة عن تسجيل 352 حادثة أمنية مختلفة، مما يعكس حالة التأهب العالي والحيوية في البيئة الرقمية للدولة، صُنفت 1 حادثة واحدة على أنها حادة الخطورة، ما يشير إلى وجود تهديدات متقدمة قد تؤثر بشكل كبير على البنية التحتية الحيوية والأمن القومي. وذكرت ان الحوادث المتوسطة بلغت 208 حادث وهذا يعني أنها قد لا ترقى إلى مستوى الخطورة العالية ولكنها لا تزال تتطلب تدخلاً أمنياً فورياً للحيلولة دون تصاعدها أما الحوادث الأقل خطورة فقد بلغت 341 حادثة، وعلى الرغم من أنها قد تكون أقل تأثيراً على المستوى الفوري، فإنها تظل مؤشراً على الحاجة المستمرة لليقظة والتحسين المستمر للأنظمة الأمنية حيث افادت التفاصيل الواردة في التقرير اشارت إلى أن الهجمات الإلكترونية التي جرى رصدها تنوعت بين البرمجيات الخبيثة والتصيد الاحتيالي، بالإضافة إلى غيرها من

الأساليب الخبيثة وتم الإبلاغ عن 58 حادثة تتعلق بالبرمجيات الخبيثة

الأمر الذي استدعى تعزيز الأنظمة الدفاعية وتحديث البرامج بشكل دوري لمنع استغلال الثغرات الأمنية وايضا تم تسجيل 87 حادثة تتعلق بالتصيد الاحتيالي عبر البريد الالكتروني، مما حتم على المؤسسات تكثيف جهود التوعية بين الموظفين لتجنب الوقوع في فخ هذه الهجمات وتم التعامل مع العدد الكبير للبلاغات معها عكس الجهود المستمرة لمراقبة الفضاء السيبراني والاستجابة السريعة للحوادث وتم رصد زيادة ملحوظة في تهديدات الأمن السيبراني خلال السنوات الأخيرة، حيث تعكس هذه التهديدات تحولات مستمرة في أساليب الهجمات وزيادة تنوع طرق التنفيذ ويتسم السيناريو الراهن بتطور سريع في مجال التكنولوجيا، مما يتيح للمهاجمين استغلال الثغرات والضعف في الأمن بطرق متقدمة ومن بين هذه التهديدات الحديثة تتضمن برامج ضارة متطورة، وهجمات التصيد الإلكتروني المستمرة، وتكتيكات هندسة التأثير الاجتماعي المتطورة ويعكس تزايد هذا التنوع والتعقيد في التهديدات السيبرانية ضرورة ملحة لتحسين القدرة على الكشف المبكر وتبني استراتيجيات أمان فعالة للتصدي لها والتي تواجه فيها البيئة الرقمية الحديثة وفيما يلي أبرز واكثر التهديدات السيبرانية شيوعا للأعوام الاخيرة في دولة الأمارات العربية المتحدة على النحو التالي :

1. الوصول غير المصرح به (Unauthorized access):

يُعد الوصول غير المصرح به واحدًا من التهديدات السيبرانية الأكثر خطورة التي تواجهها المؤسسات والأفراد على حد سواء حيث يستخدم المهاجمون أساليب متنوعة ومتطورة لاختراق الأنظمة الأمنية والحصول على البيانات الحساسة أو السيطرة على الأنظمة دون الحصول على تصريح وهذه الأفعال تشكل خطرًا كبيرًا على خصوصية الأفراد وأمن البيانات ومنه هذه الاساليب السيبرانية المنتشرة:

استخدام برامج تجسس (Spyware):

برامج التجسس هي نوع من البرمجيات الخبيثة التي تُصمم للتجسس على المستخدم دون علمه، حيث تعمل هذه البرامج في الخلفية للجهاز ويمكنها تسجيل حركات الضغطات على المفاتيح (gniggolyeK)، مما يسمح للمهاجمين بالحصول على معلومات حساسة مثل كلمات المرور وتفاصيل الحسابات المصرفية والخدمات الرقمية الاخرى فورا من غير جهد كبير

استغلال الثغرات الامنية (Exploiting security vulnerabilitities)

الثغرات الأمنية هي نقاط ضعف في نظم التشغيل أو البرامج والتطبيقات الذكية والتي يمكن للمهاجمين استغلالها حيث يبحثون عن أنظمة غير محدثة ويستغلون الثغرات

المعروفة لتنفيذ هجماتهم، مثل تثبيت البرمجيات الخبيثة أو الاستيلاء على النظام عبرها.

هجمات قواعد البيانات (SQL Injection) :

مثال الهجمات على قاعدة البيانات هي نوع من الهجمات الأمنية التي تستغل ثغرات في تطبيقات الويب لتنفيذ أوامر البيانات الحساسة لغرض تدمير البيانات، وأحيانًا السيطرة على النظام الأساسي للمضيف والخادم وحسابات المستخدم المختلفة.

استغلال كلمات مرور ضعيفة (Exploiting weak passwords):

المهاجمون يستخدمون تقنيات لتخمين أو «كسر» كلمات المرور الضعيفة أو تلك الشائعة استخدامها حيث يمكنهم أيضًا استخدام قوائم كلمات مرور تم تسريبها من خروقات أمنية أخرى لمحاولة الوصول إلى الحسابات الشخصية والحكومية.

تقنية القوة العنيفة (Brute force attacks):

تعني محاولة متكررة ومنهجية لتخمين كلمة المرور بالاعتماد على التجربة والخطأ حيث يقوم المهاجمون باستخدام برامج تحاول بمحاولات تسجيل الدخول مستخدمةً مجموعات مختلفة من الأحرف والرموز والارقام حتى يتم العثور على المزيج الصحيح.

برامج تجسس عن بعد (Remote spyware):

تُستخدم برامج التجسس عن بعد للتحكم في جهاز الضحية أو سرقة البيانات منه دون الحاجة للوصول الفيزيائي إلى الجهاز ويمكن لهذه البرامج التقاط لقطات شاشة، تسجيل الضغطات على المفاتيح، وحتى تفعيل الكاميرا والميكروفون للتجسس باستخدام برامج تجسس وتعتبر برامج التجسس من البرمجيات الخبيثة التي تُصمم للعمل في الخفاء على جهاز المستخدم والضحية ، وتقوم بمراقبة وتسجيل أنشطته دون موافقته وهذه البرامج قد تسجل ضغطات المفاتيح لالتقاط كلمات المرور، أو تتبع السلوك على الإنترنت، أو سرقة ملفات البيانات الشخصية والمالية

2. المسح/التجسس/محاولات الوصول (Aaccess attempts- Scanning):

في عالم الأمن السيبراني، يمثل المسح والتجسس ومحاولات الوصول من التهديدات الجسيمة حيث يحاول المهاجمون جمع معلومات استخباراتية عن الضحايا لاستخدامها في نشاطاتهم الخبيثة، ويستخدم المهاجمون أساليب متنوعة لتحقيق أهدافهم، بما في ذلك المسح الأمني لتحديد نقاط الضعف في الأنظمة، وقد يلجأ المهاجمون إلى تثبيت برامج تجسس عبر استغلال الضعف في الأنظمة أو من خلال الهندسة الاجتماعية لتعقب أنشطة المستخدمين وسرقة البيانات الحساسة وفيما يلي أكثر الاساليب المتبعة بالتفصيل:

المسح الشبكي (Network scanning) :

يعتمد المسح الشبكي على استخدام المسح النشط والمسح السلبي لتقديم صورة شاملة لهيكل وأمن الشبكة والمسح النشط يشمل إرسال طلبات لفحص الأجهزة والعقد المتصلة بالشبكة وفي المقابل، يعتمد المسح السلبي على تحليل حركة المرور الواردة دون القيام بطلبات نشطة وتتضمن البيانات المكتشفة من المسح الشبكي أرقام المنافذ المفتوحة، أنظمة التشغيل المستخدمة، أسماء المستخدمين في بعض الحالات، وإصدارات الخدمات والبرمجيات المشغلة على الأجهزة

المسح الضوئي gninnacs troP)):

يتم تنفيذ المسح الضوئي باستخدام أدوات متخصصة مثل (susseN، SAVnepO، tiolpsateM) وتستخدم هذه الأدوات لفحص الأنظمة وتحديد ثغرات الأمان ذات الأولوية العالية وتشمل ثغرات التحقق من الهوية، والتحقق من البروتوكولات غير الآمنة، والتسجيل غير المصرح به، وإعادة توجيه LSS ضمن الأهداف الرئيسية للمسح الضوئي.

محاولات الوصول:

تشهد محاولات الوصول غير المصرح به تنوعًا في الأساليب، حيث يتضمن ذلك الهجمات على كلمات المرور، حيث يستخدم المهاجمون تقنيات كسر كلمات المرور أو التسلل للحصول على وصول غير مصرح وتشمل هذه المحاولات استخدام ثغرات في البرمجيات، حيث يستفيد المهاجمون من الثغرات المكتشفة للوصول إلى الأنظمة دون تصريح بالإضافة إلى ذلك، تشمل الهجمات الهجينة استخدام تقنيات هندسة الاجتماع لخداع الأفراد، وتجمع هذه الهجمات بين الجوانب الاجتماعية والتقنية لتحقيق وصول غير مصرح به إلى الأنظمة

3. التصيد/التزوير/التنكر :(Phishing- Spoofing- Impersonation)

تُعَد من أكثر التهديدات السيبرانية انتشارًا في الآونة الاخيرة ، حيث يستغل المهاجمون ثقة الضحايا باستخدام تقنيات احتيالية مصممة لسرقة البيانات الشخصية والمالية وخداع الأفراد للكشف عن معلومات حساسة أو النقر على روابط ضارة كما يشمل هذا النوع من الهجمات سرقة الهويات على شبكات التواصل الاجتماعي ، حيث يمكن للمهاجمين انتحال شخصية شخص آخر للحصول على ثقة الضحايا والتلاعب بهم لأغراض ضارة ومن اكثر الأساليب المنتشرة والتي تلامس الجانب الإنساني للأمن السيبراني كالتالي :

صيد عبر البريد الإلكتروني

يعتمد صيد عبر البريد الإلكتروني على استخدام قوالب رسائل مزيفة تبدو وكأنها تأتي

من جهات موثوقة، مثل البنوك أو الشركات الكبيرة ويتم تصميم هذه الرسائل بشكل يشبه إلى حد كبير الاتصالات الرسمية للجهة المقلدة، مما يجعلها أكثر قابلية للاعتراف ويتضمن الهجوم إما روابط توجيهية إلى مواقع ويب ضارة أو ملفات مرفقة تحتوي على برامج ضارة

سرقة هويات المستخدمين:

يتم تحقيق سرقة هويات المستخدمين عبر اختراق حسابات مواقع التواصل أو حسابات البريد الإلكتروني باستخدام برامج كسر الرموز أو التصيد الإلكتروني، يمكن للهاكر الوصول إلى تفاصيل الدخول للحسابات المستهدفة ويتم توجيه هذا النوع من الهجمات غالبًا للحصول على معلومات شخصية، مثل الهوية والعناوين والمعلومات المالية.

تزوير الهوية:

يشمل تزوير الهوية بإنشاء هويات وهمية باستخدام معلومات مزورة، مثل الصور والأسماء وتفاصيل الاتصال ويستخدم المحتالون هذه الهويات للتواصل مع الأفراد والتظاهر بأنهم كيانات موثوقة أو مشاركين في أنشطة غير قانونية.

استخدام الهندسة الاجتماعية:

يتضمن استخدام هندسة الاجتماعية عبر إيهام الأفراد برسائل محكمة الصياغة والتي تستهدف العواطف أو تستغل التهديدات ويمكن أن تظهر الرسائل الاحتيالية على أنها طلبات مستعجلة أو مشاكل تتعلق بالأمان ، مما يشجع الأفراد على اتخاذ إجراءات فورية دون التحقق الدقيق.

4. هجمات وثغرات تطبيقات الويب:

تشكل تهديدًا متزايدًا، حيث يقوم المهاجمون باستغلال الثغرات الأمنية في هذه التطبيقات للوصول غير المصرح به أو حتى تدمير الأنظمة وتعد واحدة من أبرز أساليب الهجوم هي هجمات الحرمان من الخدمة الموزعة (SODD) وتشكل هذه الهجمات تمثل تحديًا كبيرًا للشركات والمؤسسات الحكومية التي تعتمد بشكل كبير على الحضور الرقمي، وأبرز اساليبها كالتالي:

هجمات الحرمان من الخدمة (DDoS):

يتم تنفيذ الهجمات عبر إرسال كميات هائلة من الطلبات إلى الخادم، مما يضغط على موارده ويجعله غير قادر على استيعاب الحمولة الكبيرة وهذا يتسبب في تقليل

جودة الخدمة للمستخدمين الشرعيين، حيث يواجهون صعوبة في الوصول إلى الموقع أو التفاعل معه بشكل فعّال

التجسس على المحتوى المشفر (XSS):

يتيح التحكم في المحتوى المشفر للمهاجم إدراج سكربتات خبيثة في صفحات الويب المستهدفة ويمكن استخدامها لسرقة معلومات المستخدمين (مثل ملفات تعريف الارتباط) أو توجيههم إلى صفحات تسجيل دخول مزيفة

عدم تحديث البرمجيات:

يتسبب عدم تحديث البرمجيات في ترك ثغرات أمنية معروفة غير مصححة، مما يفتح بابًا لاستغلالها من قبل المهاجمين مما يجبر مدراء البرامج لتحديث البرمجيات بانتظام للتأكد من أن الثغرات الأمنية السابقة قد تمت إصلاحها قبل استغلالها من قبل المهاجمين.

5. الاستخدام غير المصرح به:

يمثل تهديدًا خطيرًا حيث يسعى المهاجمون للوصول إلى البيانات أو الأنظمة لأغراض غير قانونية مثل الاحتيال أو القرصنة وهذا النوع من الهجمات يتضمن عادةً انتهاكات أمنية تتيح للمهاجمين سرقة معلومات حساسة واستغلالها بطرق غير مشروعة و يتطلب الدفاع ضد هذه الهجمات تدابير أمنية مناسبة واكثر الطرق المستخدمة والمتداولة في هذا النوع كالتالي:

الاحتيال:

يُظهر الاحتيال سلوكًا يستند إلى سرقة البيانات، حيث يُستخدم المهاجم البيانات المسروقة لتغيير تفاصيل حسابات مصرفية وتنفيذ عمليات احتيالية، ما يعرض الأفراد والمؤسسات لخسائر مالية جسيمة.

القرصنة:

يتعلق القرصنة بتسلل المهاجمين إلى الأنظمة للوصول غير المصرح به إلى البيانات أو لتعطيل الخدمات، مما يسبب تعريضًا لخطر فقدان المعلومات الحساسة والتأثير السلبي على سير العمليات

التجسس:

يتضمن التجسس استخدام المهاجمين لتقنيات جمع البيانات الشخصية بصورة غير

قانونية، ويمكن استخدام هذه المعلومات في الابتزاز أو التأثير على الأفراد والمؤسسات بشكل غير مشروع

المبحث الثاني

تحليل وتقييم مخاطر التهديدات

يُعد تحليل وتقييم المخاطر بمثابة العمود الفقري لأي استراتيجية امنية تسعى لضمان استمرارية الأعمال والحفاظ على مواردها ويتطلب هذا المنهج تبني التفكير النقدي وفهماً عميقاً لجميع العمليات والأنشطة داخل المنظمة والمؤسسة الحكومية ، بالإضافة إلى البيئة الخارجية التي تعمل فيها ويشمل التحليل تحديد المخاطر المحتملة، سواء كانت مالية، تقنية، قانونية، أو حتى مرتبطة بالسمعة المؤسسية، ومن ثم تقييمها من حيث الاحتمالية والأثر، والتقييم الدقيق يقود إلى تصنيف المخاطر إلى قابلة للتجنب، مقبولة، أو تلك التي يجب التحوط ضدها ليساعد هذا التصنيف في توجيه الموارد المحدودة نحو التهديدات الأكثر جدية والفرص الأكثر قيمة ، وتُستخدم هذه المعلومات لتشكيل سياسات المؤسسات وإجراءاتها التشغيلية، وتعزيز الشفافية داخل المؤسسة ومع أصحاب المصلحة من الشركاء الداخليين والخارجيين

ومن الأساسيات أن تكون عملية تحليل المخاطر مستمرة وديناميكية لتعكس التغيرات السريعة في بيئة الأعمال، من خلال مراجعة الخطط بانتظام وتحديثها لضمان استجابة فعالة لأي حدث طارئ وتتضمن هذه الخطط، على سبيل المثال، إجراءات الإخلاء، خطط الاستمرارية للأعمال ، واستراتيجيات التعافي من الكوارث ، وإدارة المخاطر ليست فقط عن تجنب الخسائر والسمعة المؤسسية ، بل تشمل أيضاً التعرف على الفرص التي يمكن أن تحسن من مكانة المؤسسة وتنافسيتها وتقييم المخاطر يمكن أن يكشف عن مجالات للتحسين، أو تبني تقنيات جديدة قد تقود إلى نمو المؤسسة ويمكن لهذا النهج المتوازن ضمان للمؤسسات الحكومية أن لا تتخذ فقط إجراءات تحفظية، بل تبحث أيضًا عن طرق للتوسع والابتكار وبالتالي تحليل وتقييم المخاطر يجب أن يُنظر إليه كجزء لا يتجزأ من العمليات اليومية لأي مؤسسة حكومية مما يساهم في بناء ثقافة الوعي بالمخاطر ويشجع على النظرة الاستباقية للتحديات والفرص، ويؤدي إلى اتخاذ قرارات أكثر استنارة وتحقيق مستويات أعلى .

ويعتبر تحليل وتقييم المخاطر عملية حيوية تساهم في تحصين المنظمات الحكومية ضد الأحداث غير المتوقعة وتزويدها بالقدرة على التكيف والصمود في وجه الصدمات

وتتضمن هذه العملية تحديد الأصول الحيوية للمنظمة والتهديدات المحتملة التي يمكن أن تؤثر عليها، ومن ثم تحليل هذه المخاطر من حيث الاحتمالية والتأثير ويساعد هذا التقييم في تحديد أولويات الإدارة وتوجيه الاستثمار في الأمن والحماية إلى الأماكن الأكثر احتياجًا.

يسهم التقييم الجيد للمخاطر في تطوير خطط استجابة مرنة تتيح للمنظمة التعامل مع الحوادث بفعالية وتقليل الأضرار ، كما يعزز القدرة على الاستجابة السريعة والفعالة في حالات الطوارئ، مما يضمن استمرارية الأعمال وحماية الموارد البشرية والمادية ، علاوة على ذلك، تلعب عملية التحليل والتقييم دورًا رئيسيًا في تطوير ثقافة الوعي بالمخاطر داخل المنظمة من خلال تدريب العاملين وتوعيتهم بالمخاطر المحتملة وكيفية التعامل معها، وتُعزز المؤسسات من مرونتها وقدرتها على التكيف مع التغيرات وبناء على منهجية تحليل المخاطر، يمكن للمنظمات الحكومية من تطوير استراتيجيات تأمين تنافسية وشاملة تحمي ليس فقط الأصول المادية، بل أيضًا المعلومات الحساسة والسمعة المؤسسية وتتضمن هذه الاستراتيجيات تدابير الحماية الإلكترونية، الأمن الفيزيائي، وسياسات الخصوصية والامتثال ، ويمكن القول إن تحليل وتقييم المخاطر يشكل ركنًا أساسيًا في إدارة المؤسسات الريادية، وهو أداة ضرورية لتعزيز الكفاءة والفعالية، وضمان النمو المستدام والنجاح طويل الأمد وبالتنسيق مع الشركاء في كل القطاعات وتعد التهديدات السيبرانية من المخاطر الرئيسية التي تواجه المؤسسات الحكومية في الامارات في الوقت الحالي ، حيث أصبحت الهجمات الإلكترونية أكثر تعقيداً وتطوراً، مستهدفة الأصول والمعلومات الرقمية التي تعتمد عليها معظم الحكومات في أداء أعمالها ومن اجل ذلك، تم التركيز في هذا المبحث على تحليل اكثر هذه التهديدات الخمس تكرارا واهمية وهي كالتالي

-الوصول غير المصرح به: سبب التركيز عليها لأنها من أكثر التهديدات شيوعًا وخطورة في القطاعات الحكومية

- **المسح والتجسس:** سبب التركيز لقدرتها على جمع معلومات حساسة تستخدم لاحقًا في هجمات متقدمة على الانظمة الحكومية.
- **التصيد والتزوير:** سبب التركيز لسرعة انتشاره الواسع وتأثيره السلبي على سمعة المؤسسة الحكومية.
- **هجمات تطبيقات الويب:** سبب التركيز عليه نظرًا لاعتماد الكثير من الأعمال الحكومية على تطبيقات الويب ومواقعها في الشبكة العنكبوتية.
- **الاستخدام غير المصرح به:** سبب التركيز عليه لما يسببه من إهدار للموارد التقنية

والمالية وإمكانية استغلالها في أنشطة غير قانونية على المؤسسة.

سنقوم بتقييم شامل لاحتمالية حدوث التهديدات ومستوى تأثيرها على موارد المؤسسة الحساسة، وذلك بهدف تحديد الأولويات في التعامل مع كل تهديد وسيشمل التقييم تحليل احتمالية حدوث التهديدات بناءً على البيانات التاريخية وتحليلات الأمن والحماية للمعلومات ، مع تقييم تأثيرها المحتمل على بيانات المؤسسة وأنظمتها وخدماتها بناءً على نتائج التقييم، سنحدد الأولويات ونضع الضوابط والإجراءات اللازمة لتقليل مخاطر هذه التهديدات في المستقبل ويتضمن النهج الشامل أيضًا تحسين قدرة المؤسسة على الاستجابة السريعة والفعّالة للطوارئ، وضمان تنفيذ إجراءات التخفيف بفعالية لضمان استمرارية العمليات الأساسية

التهديد السيبراني الوصول غير المصرح به

فهم التهديد السيبراني:

يشير الوصول غير المصرح به إلى قيام شخص غير مخول قانوناً بالدخول إلى نظام حاسوبي أو شبكة إلكترونية أو الولوج إلى بيانات حساسة مخزنة داخلها ويعد هذا التهديد من أخطر التهديدات السيبرانية التي تهدد خصوصية البيانات وسلامتها ، حيث يمكن للمخترق تدمير البيانات أو سرقتها أو التلاعب بها ، ويمكن أن يتم ذلك عن طريق التجسس والاختراق عبر إيجاد ثغرات أمنية في نظام الحماية الإلكترونية أو عبر توجيه برمجيات خبيثة أو الاستفادة من أخطاء المستخدمين مثل تسريب كلمات المرور والبيانات الشخصية ويمكن أن يؤدي إلى انتهاك خصوصية المعلومات لفترات طويلة دون أن يكتشف أمره.

تصنيف التهديد السيبراني:

يمكن تقسيم أنواع التهديدات المرتبطة بالوصول غير المصرح به إلى الفئات الرئيسية التالية

الاختراق عن بُعد: وهو اختراق أجهزة الضحية والتحكم بها عن بعد عبر شبكة الإنترنت، مثل استغلال برامج التحكم عن بعد مثل reweiVmaeT أو ثغرات أمنية في بروتوكولات الاتصال عن بعد.

البريد الإلكتروني الاحتيالي: حيث يرسل المهاجم رسائل إلكترونية تحتوي على روابط أو مرفقات خبيثة بهدف خداع المستخدم وجمع معلوماته أو تسريب بياناته: مثل رسائل التصيد الاحتيالي.

استغلال ثغرات البرمجيات: مثل استهداف ثغرات معروفة في أنظمة التشغيل أو تطبيقات الويب للحصول على وصول غير مصرح به

الهندسة الاجتماعية: تعتمد على خداع وتضليل المستخدمين لجمع معلومات حساسة منهم أو حملهم على تنفيذ إجراءات غير آمنة مثل كشف كلمات المرور

الشبكات غير الآمنة: استهداف الأجهزة والشبكات غير المحمية أو ذات الإعدادات الافتراضية مما يسهل الاختراق

الأجهزة الملوثة: نشر برامج خبيثة على أجهزة الضحايا تسمح بالتحكم والوصول غير المصرح به

تقدير للتأثير المحتمل للوصول غير المصرح به على توفير الخدمات الحكومية الرقمية:

يمكن لحادثة الوصول غير المصرح به أن تؤدي إلى توقف مؤقت أو طويل المدى للخدمات الحكومية الرقمية، حيث يمكن للمخترق تدمير بيانات الخدمة أو الموقع الإلكتروني، ما يتطلب إعادة بناء البنية التحتية ، كما قد تتعرض بيانات المتعاملين للسرقة ما قد يسبب مخاوف من الخصوصية وفقدان الثقة بالحكومة حيث يمكن تقدير أن هجوم الوصول غير المصرح به سيؤدي بشكل مباشر إلى عرقلة تقديم الخدمات لفترة زمنية تتراوح بين أيام إلى أشهر حسب حجم الضرر وهذا بالإضافة إلى تكاليف إعادة البناء وخسائر غير مباشرة ناجمة عن فقدان الثقة وسمعة الحكومة ، كما يمكن أن تتعرض الحكومة لدعاوى قانونية وغرامات مالية بسبب انتهاكات الخصوصية

الحوادث السيبرانية للتهديد الوصول غير المصرّح به في السنوات الأخيرة:

في عام 2020 ، إحدى أبرز حوادث الاختراق الحقيقية المرتبطة بالوصول غير المصرح به هي حادثة اختراق شركة (sdniWraloS الأمريكية للبرمجيات، حيث استطاعت مجموعة من القراصنة المرتبطين مع الاستخبارات الروسية من الوصول إلى شبكة الشركة وإدخال برمجيات خبيثة مخفية ضمن تحديثات منتجاتها، وهذه البرمجيات الخبيثة انتشرت فيما بعد إلى آلاف عملاء الشركة من المؤسسات الحكومية والشركات الكبرى، مما سمح للمهاجمين بالوصول غير المصرح به لشبكاتهم وسرقة كم هائل من البيانات الحساسة وتُعد هذه الحادثة واحدة من أكبر عمليات الاختراق عبر سلسلة التوريد في التاريخ .

التهديد السيبراني: المسح والتجسس

فهم التهديد السيبراني للمسح والتجسس على الخدمات الحكومية الرقمية:

المسح والتجسس السيبراني على الخدمات الحكومية الرقمية يشير إلى قيام أطراف غير مصرح لها بجمع المعلومات الحساسة والبيانات الشخصية للمواطنين أو موظفين حكوميين

في الدولة من قواعد البيانات ونظم المعلومات الحكومية دون إذن، ويهدف المخترقون من خلال ذلك للحصول على معلومات استخباراتية وتستخدم لأغراض غير مشروعة مما يشكل تهديداً خطيراً للخصوصية والأمن الوطني بالدولة

تصنيف التهديد السيبراني للمسح والتجسس الخدمات الحكومية الرقمية:

تتنوع أساليب وطرق المسح والتجسس السيبراني على الخدمات الحكومية الرقمية، والتي يمكن تصنيفها إلى

الاختراق عبر البريد الإلكتروني: وذلك من خلال إرسال رسائل بريد إلكتروني مزيفة تحتوي على روابط أو ملفات ملحقة مخربة تمكن المخترق من الوصول غير المشروع لأنظمة الحكومة

استغلال ثغرات الأمان: حيث يتم الاعتماد على ثغرات أمنية معروفة في برامج أو أنظمة التشغيل تستخدمها الحكومة مثل deelbtraeH للدخول غير المصرح به.

استخدام أدوات التجسس السيبرانية: مثل برامج التجسس أو «الروتكيت» التي يتم تركيبها عن بعد على أنظمة الحكومة للولوج المستمر وسرقة البيانات المهمة فيها تقدير التأثير المحتمل للمسح والتجسس على توفير الخدمات الحكومية الرقمية:

يمكن لحادثة المسح والتجسس السيبراني أن تؤدي إلى سرقة بيانات حساسة أو سرية لدى الحكومة ، حيث يستطيع المخترق الاطلاع على معلومات المواطنين مثل أرقام الهوية والرقم الضريبي والبيانات الصحية وغيرها ويمكن تقدير أن هجوم المسح والتجسس قد يؤثر سلبًا على مستوى الثقة لدى المواطنين والوافدين بخصوصية بياناتهم وسريتها لدى الحكومة ، كما قد يؤدي في بعض الحالات إلى تعليق بعض الخدمات أو إعادة هيكلة أنظمتها الأمنية بالإضافة إلى خسائر مالية قد تنجم عن دفع تعويضات أو غرامات كما ستواجه الحكومة تكاليف كبيرة لإعادة تأمين وحماية نظمها المعلوماتية وتصليح أي أضرار وعلى المدى الطويل، وقد تتعرض لغرامات قضائية أو خسائر متمثلة في تعطيل بعض الخدمات أثناء عمليات التأمين هذا بالإضافة إلى التكاليف غير المباشرة المترتبة على استعادة الثقة والجهود المبذولة لإعادة البناء لحوادث السيبرانية للتهديد للمسح والتجسس في السنوات الأخيرة ويمكن توقع حدوث مجموعة من التأثيرات السلبية المحتملة نتيجة تعرض الخدمات الحكومية الإلكترونية لتهديد المسح والتجسس، حيث تعرضت العديد من الهيئات الحكومية لعدد من حوادث المسح والتجسس خلال السنوات الأخيرة ومن أبرز هذه الحوادث:

في عام 2015، تمكن مجهولون من اختراق حساب البريد الإلكتروني الشخصي الخاص بهيلاري كلينتون وهي كانت وزيرة الخارجية الأمريكية آنذاك حيث استطاع الهاكر الوصول إلى العديد من الرسائل الشخصية والحكومية الخاصة بكلينتون، بما في ذلك بعض الأوامر والتعليمات السرية حيث لم يتم الكشف عن هوية الهاكرز، لكن تقارير صحفية أشارت إلى أنهم ربما يعودون إلى كيانات حكومية أجنبية وتسبب هذا الاختراق بجدل كبير حول إجراءات الأمن السيبراني المتبعة لدى وزارة الخارجية الأمريكية وكما أثر هذا الحادث سلبًا على حملة كلينتون الرئاسيـــة فيما بعد .

التهديد السيبراني التصيد والتزوير

فهم التهديد السيبراني:

التصيد والتزوير السيبراني هو إحدى أكثر طرق الاحتيال السيبراني شيوعاً، حيث يتم من خلاله إنشاء نسخ مزيفة ومواقع وهمية تشبه المواقع الحكومية مثل المصارف أو الوزارات الخدمية وتستهدف الحصول على معلومات سرية مثل أرقام الحسابات وبطاقات الائتمان وأرقام الضمان الاجتماعي والخ، كما يتم استخدام عناوين بريد إلكتروني مزيفة تشبه تلك الخاصة بالجهات الحكومية لإرسال رسائل احتيالية ونشر روابط مضللة ما يشكل تهديدًا مباشراً لبيانات الهوية والحسابات المالية للمواطنين والمقيمين في الدولة .

تصنيف التهديد السيبراني التصيد والتزوير على الخدمات الرقمية الحكومية:

يمكن تصنيف طرقها حسب طريقة الاستهداف والأسلوب المتبع على النحو التالي:

التصيد برسائل بريد إلكتروني احتيالية: تحتوي على روابط أو ملفات مضللة تستهدف بيانات الدخول لحسابات حكومية.

استخدام مواقع وهمية (مماثلة): تشبه المواقع الرسمية للخدمات الحكومية لجذب الضحايا

تقدير التأثير المحتمل التصيد والتزوير على توفير الخدمات الحكومية الرقمية:

يمكن توقع تأثيرات سلبية كبيرة لعمليات التصيد والتزوير على الخدمات الحكومية الرقمية، منها:

- فقدان ثقة المواطنين وعدم الاعتماد على الخدمات الإلكترونية بشكل كلي.
- سرقة هويات أو بيانات شخصية للمواطنين والمقيمين وقد تستخدم في عمليات احتيال لاحقة.
- تكبد الحكومة تكاليف كبيرة لإصلاح الثغرات الامنية وحماية البيانات.

- إمكانية توقف أو تعطل بعض الخدمات أثناء معالجة حوادث التصيد التي حدثت.
- الحوادث السيبرانية للتهديد التصيد والتزوير في السنوات الأخيرة:

حادثة استهداف موقع ضريبة مبيعات تكساس الأمريكي لهجوم تصيد كبير عام2019يعتبر موقع دائرة ضرائب مبيعات ولاية تكساس الأمريكية أحد أهم المواقع الحكومية لتقديم بيانات الضرائب الإلكترونية ، في شهر يناير 9102، تعرض الموقع لهجوم تصيد إلكتروني كبير من خلال موقع محاكاة مزيف وتمكن المهاجمون من جذب آلاف الضحايا إلى إدخال بياناتهم الشخصية والضريبية على الموقع الوهمي ، أدى الحادث إلى سرقة هويات العديد من المواطنين وبياناتهم المالية، ما تسبب في خسائر كبيرة .

التهديد السيبراني هجمات تطبيقات الويب

فهم التهديد السيبراني:

تشير هجمات تطبيقات الويب إلى الهجمات التي تستهدف الوصول غير المصرح به إلى تطبيقات ونظم الويب المستخدمة في تقديم الخدمات الحكومية عبر الإنترنت وتتضمن هذه التطبيقات مواقع الحكومة والمنصات الرقمية المختلفة حيث يحاول المهاجمون الاختراق من خلال استغلال ثغرات أمنية بهدف الوصول غير المصرح به لقواعد البيانات الحكومية أو معلومات المستخدمين مثل بياناتهم الشخصية والمالية كما قد تستهدف هذه الهجمات إلحاق الضرر بالبنى التحتية التقنية للحكومة أو إسقاط المواقع ومنصات الخدمات بشكل عام، وتشكل هجمات تطبيقات الويب تهديداً للخصوصية والأمن السيبراني للقطاع الحكومي بشكل مستمر .

تصنيف التهديد السيبراني هجمات تطبيقات الويب:

هذه بعض أنواع تصنيف هجمات تطبيقات الويب منها استغلال ثغرات الأمان في التطبيقات ومن من أبرزها هجمات اختراق شفرة جافاسكربت SSX حيث يتم حقن رموز برمجية خبيثة عبر المتصفح تسمح بتنفيذ أوامر على الخادم كما تشمل noitcejnI LQS حيث يتم إدخال استعلامات نصية للولوج غير المشروع قاعدة البيانات

الهجمات الموزعة: مثل هجمات رفض الخدمة SoD حيث يتم تعطيل الموقع بزيادة الطلبات بشكل مفرط لاستنزاف الموارد أو التوزيعية SoDD والتي تستهدف الموقع من عدة مصادر لهدف اسقاط الموقع الحكومي الرئيسي ويعتبر من أخطر الادوات الشائعة حاليًا.

تطبيق برمجيات تجسس: مثل فتح سلسلة أوامر روتكت تسمح للمهاجم بالولوج طويل الأمد للنظام لتنفيذ أوامر وسرقة البيانات الحكومية من غير استشعار من الخوادم الحكومية حولها.

تقدير التأثير المحتمل هجمات تطبيقات الويب على توفير الخدمات الحكومية الرقمية:

يمكن توقع حدوث عواقب سيئة جداً ناتجة عن هذه الهجمات، مثل تعطيل الوصول إلى الخدمات الحيوية عبر الإنترنت لفترات طويلة قد تؤثر على راحة المواطنين والمقيمين وسير العمل الحكومي كما يمكن أن تتسبب بسرقة معلومات حساسة للجهات الحكومية أو المواطنين مثل البيانات المالية والشخصية ما قد يسبب مخاطر أمنية وقانونية كبيرة، كما سيترتب عليها تكبد تكاليف باهظة لإصلاح أوجه القصور الأمنية في الانظمة الخدمية.

الحوادث السيبرانية للتهديد هجمات تطبيقات الويب حدثت في السنوات الأخيرة:

في عالم الامن السيبراني، وتحديدًا فيما يتعلق بتهديدات تطبيقات الويب، شهدت السنوات الأخيرة العديد من الحوادث البارزة حيث يُعد اختراق بيانات إيكوفاكس في عام 2017 أحد الأمثلة الملحوظة، حيث تم اكتشاف الاختراق في يوليو 7102، وأدى إلى تسريب معلومات حساسة لنحو 741 مليون فرد، بما في ذلك الأسماء والأرقام الاجتماعية وتواريخ الميلاد تجلى استغلال المهاجمين لثغرة في إطار تطبيق الويب Apache Struts، بالتحديد الثغرة EVC-7107-5638، والتي سمحت بتنفيذ الشيفرة عن بُعد، مما أتاح الوصول غير المصرح به إلى أنظمة إيكوفاكس وكانت هذه الحادثة تسلط الضوء على أهمية تحديث الثغرات بشكل فوري وفعّال لتعزيز أمان تطبيقات الويب في القطاعات الحكومية

التهديد السيبراني الاستخدام غير المصرح به

فهم التهديد السيبراني الاستخدام غير المصرح به على الخدمات الرقمية الحكومية:

الاستخدام غير المصرح به يعبر عن استنزاف موارد وخدمات المؤسسات الحكومية الرقمية بطرق غير قانونية أو خارج حدود الصلاحيات المخولة ويشكل هذا التصرف تهديدًا جسيمًا على أمان وسرية البيانات والمعلومات الحكومية ويمكن لهذا الاستخدام الغير المصرح به أن يؤدي إلى تسريب البيانات أو تلفها، بالإضافة إلى احتمال استغلال الخدمات الحكومية في أنشطة غير قانونية على سبيل المثال، يمكن للمهاجمين الذين يستخدمون طرق الوصول غير المصرح به أن يتسببوا في اختراق أنظمة الحكومة الرقمية، مما يتيح لهم الوصول غير المسموح به إلى المعلومات الحساسة ويمكن لهؤلاء الأفراد أو الكيانات أيضًا استخدام هذا الوصول لتحقيق أهداف غير قانونية، مثل تزوير الهوية أو استنساخ البيانات لأغراض احتيالي كبير.

تصنيف التهديد السيبراني الاستخدام غير المصرح به على الخدمات الرقمية الحكومية:

يُمكن تقسيم أشكال الاستخدام غير المصرح به للخدمات الحكومية الرقمية إلى عدة فئات رئيسية

استخدام بيانات المواطنين والمقيمين في أغراض شخصية أو تجارية من قِبل موظفين حكوميين: يتضمن هذا النوع من الاستخدام غير المصرح به حالات حيث يقوم الموظفون الحكوميون بالوصول غير القانوني إلى بيانات المواطنين والمقيمين واستخدامها لأغراض شخصية أو تجارية على سبيل المثال، قد يقوم موظف ببيع البيانات الشخصية لشركات التسويق أو استخدامها لتحقيق مكاسب مالية خاصة.

الوصول إلى الأنظمة الحكومية من قِبل متسللين خارجيين للحصول على بيانات حساسة: تشمل هذه الفئة الهجمات الإلكترونية من قبل متسللين أو جهات خارجية تسعى لاختراق الأنظمة الحكومية الرقمية للوصول إلى بيانات حساسة مثل المعلومات الشخصية، السجلات المالية، أو المعلومات الأمنية القومية المهمة.

استخدام الخدمات العامة مثل الرعاية الصحية أو المنافع من قِبل أشخاص غير مؤهلين: هذا النوع يشير إلى حالات حيث يقوم أفراد بالتظاهر بأنهم مؤهلون للحصول على خدمات حكومية معينة مثل المساعدات الاجتماعية، التأمينات الصحية، أو غيرها من المنافع دون أن يكون لهم الحق الفعلي في ذلك

تزوير الوثائق الرسمية أو بيانات الهوية للحصول على خدمات حكومية: يشمل هذا الفعل إنتاج وثائق مزورة مثل جوازات السفر، بطاقات الهوية، شهادات الميلاد أو أي وثيقة أخرى تستخدم لإثبات الهوية أو الأهلية للحصول على خدمات حكومية بطريقة غير مشروعة

استغلال ثغرات أمنية في المنصات الرقمية للحصول على بيانات شخصية: يتعلق هذا النوع من الاستغلال بالأشخاص الذين يبحثون عن ويستغلون الضعف في البرمجيات والأنظمة الحكومية الرقمية للوصول إلى بيانات شخصية أو معلومات سرية قد يشمل ذلك استغلال استخدام بيانات المواطنين في أغراض شخصية أو تجارية من قِبل موظفين حكوميين وقد يشمل ذلك بيع البيانات لطرف ثالث، استخدام المعلومات لكسب ميزة في تعاملات تجارية خاصة، أو حتى لأغراض الابتزاز والفساد

تقدير التأثير المحتمل الاستخدام غير المصرح به على توفير الخدمات الحكومية الرقمية:

يمكن أن يؤثر الاستخدام غير المصرح به للخدمات الحكومية الرقمية سلباً على توفير تلك الخدمات وجودتها من عدة جوانب

- تعطيل الخدمات وتوقفها بسبب الاختراقات والهجمات السيبرانية: يمكن أن يؤدي اختراق الأنظمة السيبرانية إلى تعطيل الخدمات الحيوية، مما يتسبب في توقف العمليات اليومية وتأثير سلبي على الفعالية العامة للمؤسسة.
- تدني ثقة المواطنين والمقيمين بالخدمات الإلكترونية وعزوفهم عن استخدامها: الاختراقات تسفر عن تدهور الثقة في الأمن السيبراني، مما يؤدي إلى استياء المستخدمين وتراجع اعتمادهم على الخدمات الإلكترونية.
- تكاليف إضافية لاستعادة نظم المعلومات وتعويض المتضررين: يتطلب استعادة النظم وتعويض المتضررين تخصيص موارد إضافية، مما يتسبب في تكاليف مالية ووقتية إضافية للمؤسسة.
- إتلاف البيانات وفقدانها مما يؤثر على تقديم الخدمات: فقدان البيانات يعرض المؤسسة لخسائر لا رجعة فيها، مما يؤثر على فعالية تقديم الخدمات ويتطلب جهودًا كبيرة لاستعادة أو إعادة إنشاء تلك البيانات.
- تدني جودة الخدمات بسبب استغلال الثغرات الأمنية: استغلال الثغرات الأمنية يمكن أن يؤدي إلى تدني جودة الخدمات المقدمة، مع تأثير سلبي على تجربة المستخدم وسمعة المؤسسة.
- تعطيل سير العمل الحكومي وإرباك الإجراءات الإدارية فيها: يمكن أن يسفر الاختراق عن تعطيل سير العمل الحكومي وإرباك الإجراءات الإدارية، مما يؤثر على القدرة على تقديم الخدمات بشكل فعال وسلس.

الحوادث السيبرانية للتهديد الاستخدام غير المصرح به في السنوات الأخيرة:

أحد الحوادث السيبرانية البارزة التي شهدت استخدامًا غير مصرح به على الخدمات الحكومية الرقمية كانت حادثة «واناكراي» (yrCannaW) في عام 7102 هذه الهجمة الإلكترونية استهدفت نظام الصحة الوطني في المملكة المتحدة ، مما أدى إلى تعطيل أنظمة المستشفيات وتشفير البيانات وتسببت هذه الهجمة في تأثير كبير على تقديم الرعاية الصحية، حيث تعطلت العديد من الخدمات الحيوية، مثل جداول العمليات وإدارة الملفات الطبية ،المهاجمون قاموا باستغلال ثغرة في نظام تشغيل مايكروسوفت ويندوز التي لم يتم تحديثها بشكل صحيح، مما سمح لبرنامج الفدية الخبيث بالانتشار بشكل سريع وتم مطالبة المستخدمين بدفع فدية إلكترونية لاستعادة الوصول إلى بياناتهم ، وعلى اثرها تم تسليط الضوء على أهمية تحديث الأنظمة الرقمية وتعزيز الوعي الأمني، وضرورة اتخاذ إجراءات فعالة للوقاية من تبعات هجمات الاستخدام غير المصرح به في القطاعات الحكومية

في ختام مبحث تحليل وتقييم مخاطر التهديدات، يظهر أن هذه العملية أساسية لفهم التحديات التي تواجه المؤسسة وتحديد الأفضليات في مواجهتها حيث تم تسليط الضوء على تأثيرات متنوعة قد تنشأ نتيجة لتهديدات الامن والحماية ، وهو ما يشكل الخطوة الأولى نحو تطوير استراتيجيات فعّالة للتعامل مع تلك التحديات ولتحقيق فعالية في إدارة المخاطر يتطلب تفهمًا عميقًا للاحتماليات وتأثيرات التهديدات المختلفة، مما يمكننا من وضع خطة شاملة لتقليل الفرص المتاحة للهجمات وتقليل الأضرار المحتملة في حال وقوعها مع تطور تهديدات الأمان باستمرار، يظل التحليل والتقييم وسيلة دائمة لمواكبة التغيرات وضمان استمرار فعالية استراتيجيات الأمان، مما يتطلب من المؤسسة الحكومية البقاء حذرة والتزامًا بمتابعة أحدث التطورات وتحسين استعدادها للتعامل مع التهديدات المستقبلية

الفصل الثالث

استراتيجيات وتدابير الأمن السيبراني في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ

يتضمن هذا الفصل مبحثين أساسيين حيث يُعالج المبحث الأول الاستراتيجيات والتدابير الوقائية الناجحة للتعامل مع التهديدات السيبرانية الناشئة في الخدمات الرقمية، أمّا المبحث الثاني، فيلقي الضوء على توفير التوعية السيبرانية المستمرة والتطوير المستمر للموظفين لتحسين مستوى الأمن السيبراني

المبحث الأول

- **الاستراتيجيات والتدابير الوقائية للتعامل مع التهديدات السيبرانية الناشئة في الخدمات الرقمية الحكومية**

1. سياسات الأمن السيبراني والإجراءات الإدارية :

يُعد تحليل التهديدات السيبرانية هو عملية شاملة ومنهجية تهدف إلى تحديد وتقييم التهديدات المحتملة التي تؤثر على الموارد الرقمية لمؤسسات الحكومية ويعتبر هذا التحليل جزءًا لا يتجزأ من عملية وضع صنع السياسات الأمنية السيبرانية في الحكومات ولعدة أسباب:

أولاً : يوفر فهم استراتيجي دقيق للبيئة السيبرانية، حيث يمكن للمؤسسات أن تكتسب رؤية واضحة حول التهديدات الحالية والمستقبلية وأهداف المهاجمين وأساليبهم والثغرات الأمنية الموجودة في المؤسسة.

ثانيًا : يساعد في تحديد الثغرات الأمنية واكتشاف النقاط الضعيفة في البنية التحتية السيبرانية للمؤسسة، مما يمكنها من اتخاذ إجراءات استباقية لمعالجة هذه الثغرات بشكل دائم.

ثالثاً : يساعد في التكيف مع التغيرات المستمرة في التهديدات السيبرانية، حيث يساعد التحليل المستمر على مواكبة أحدث التكتيكات والتقنيات المستخدمة من قبل المهاجمين مع مزامنته في تطوير اساليب الدفاع السيبرانية المضاده لها.

وأخيرًا : يدعم اتخاذ القرارات الاستراتيجية السليمة من خلال توفير بيانات مهمة يمكن استخدامها في تخصيص الموارد بشكل فعال وضمان توافق الاستثمارات الأمنية مع مستوى التهديدات الفعلية الحاصلة والتي قد تحصل في المستقبل القريب

يُعتبر **تقييم المخاطر للسياسات الأمنية** خطوة حاسمة لفهم السياق الذي تعمل فيه السياسات وتحديد الأماكن التي يجب تعزيزها ويشدد على أهمية هذه العملية لتقييم المخاطر يسهم في رؤية شاملة للتهديدات المحتملة ويُمكن من وضع أولويات فعّالة لتحسين الأمن ، يُظهر التقييم الدوري للمخاطر كيف يمكن تحسين السياسات الأمنية بشكل مستدام ويجب أن يُركز على تحديد الأولويات بناءً على تأثير المخاطر واحتمال حدوثها، حيث يقول تقديم تقييم دوري للمخاطر يُمكن من تعزيز السياسات الأمنية بتحديد الأولويات الفعّالة لتعزيز مستوى الحماية ويُسلط التقييم الدوري للمخاطر الضوء على ضرورة التكيف مع التحديات المتغيرة في مجال الأمن السيبراني ويعزز هذا النهج من القدرة على التصدي للتهديدات الجديدة وتحسين الاستعداد للتغييرات في البيئة السيبرانية ويُظهر التركز على تحديد الأولويات كفعل أساسي في تحسين السياسات الأمنية، حيث يمكن أن يوجه تخصيص الموارد بشكل أكثر فعالية وتقدم هذه العملية فرصة لتحديد المجالات التي تحتاج إلى تعزيز وتحسين فعالية الحماية ويُشير التأكيد على تعزيز مستوى الحماية إلى أهمية التقييم المستمر للمخاطر وضبط السياسات استنادًا إلى التحديات المستجد ويساهم ذلك في بناء أنظمة أمان قوية ومستدامة.

سياسات التحكم في الوصول تُعد جزءًا أساسيًا من إطار الأمن السيبراني لأي منظمة أو نظام وتهدف هذه السياسات إلى تنظيم وتحديد الوصول إلى الموارد والبيانات الحساسة، مما يعزز الحماية من التهديدات السيبرانية ويقوم تصميم وتنفيذ سياسات التحكم في الوصول على أساس مبادئ الحاجة والمسؤولية، حيث يتم تحديد الصلاحيات بناءً على احتياجات الفرد ودوره في المؤسسة وتشمل سياسات التحكم في الوصول قواعد محددة لتحديد من يحق له الوصول إلى المعلومات والموارد وفقًا للمبادئ الامنية ويُفضل أيضًا

تضمين آليات التحقق من الهوية للتأكد من أن الشخص الذي يحاول الوصول هو الشخص المصرح له، مما يعزز مستوى الأمن والحماية للمعلومات بالمؤسسة .

من الجوانب الأخرى، يُحدد تنفيذ سياسات التحكم في الوصول كيفية إدارة الوصول للمستخدمين داخل المؤسسة، بما في ذلك تحديد الصلاحيات وتحديثها أو إلغائها عند تغير الوظائف أو المسؤوليات ويتضمن ذلك أيضًا توثيق ورصد الأنشطة المرتبطة بالوصول لتعزيز فهم المؤسسة للاستخدامات غير المصرح بها وتعزيز القدرة على استدراك أي انتهاكات أمنية قد تحدث، ولتحقيق الأمن السيبراني يتطلب تنفيذ سياسات صارمة للتحكم في الوصول وضبط إدارة الهويات لتحسين أمن البيانات.

يُفيد استخدام أنظمة إدارة الهويات والتوثيق من الشخص في تحقيق توازن بين التأمين وسهولة الوصول وتُشير الآليات المتعددة العوامل إلى الطبقة الإضافية للأمان والتي يمكنها تعزيز قدرة النظام على مقاومة الوصول غير المصرح به، ولحقيق الأمن السيبراني يعتمد على تنفيذ سياسات صارمة للتحكم في الوصول واستخدام آليات مصادقة متعددة العوامل لتعزيز الأمان.

2. تعزيز البنية التحتية لتكنولوجيا المعلومات:

1.2 تقنين الأجهزة والبرمجيات:

تقنين الأجهزة والبرمجيات يلعب دورًا حاسمًا في استراتيجية الأمن السيبراني للخدمات الرقمية الحكومية ويركز هذا النهج على توفير تحديثات دورية للأنظمة والبرمجيات لتعزيز الأمان وسد الثغرات الأمنية المعروفة حيث عند اكتشاف ثغرة أمنية جديدة في الأنظمة أو البرمجيات، يتم توفير تحديثات أمنية لسد هذه الثغرة ومنع استغلالها بشكل سيئ وعند تحديث الأنظمة والبرمجيات بشكل منتظم سيساهم في تحسين الأمن السيبراني، ويتم على اثر ذلك تصحيح الثغرات الأمنية المعروفة والتعامل مع التهديدات الجديد ، يتم تطوير هذه التحديثات بواسطة مزودي التكنولوجيا ويتم توفيرها للمستخدمين عبر التحديثات الأمنية باستمرار وبالتالي، تقوم الجهات الحكومية والمؤسسات بالاعتماد على هذه التحديثات لضمان استمرارية الأمن السيبراني

بالإضافة إلى ذلك، يتم تقنين استخدام التكنولوجيا لمواكبة التطورات الأمنية مما يعني ذلك استخدام البرمجيات والأجهزة ذات التراخيص القانونية والمعتمدة وعند استخدام برمجيات غير مرخصة أو أجهزة غير قانونية، يمكن أن ينشأ خطر قانوني وأمني على المؤسسة وقد تكون هذه البرمجيات والأجهزة غير موثوقة وقد تحتوي على ثغرات أمنية قد تستغلها الهجمات السيبرانية ، بصفة عامة، تقنين الأجهزة والبرمجيات يعزز الأمان

السيبراني للخدمات الحكومية الرقمية يساعد في منع الهجمات السيبرانية وتقليل المخاطر الأمنية بالاعتماد على تحديثات الأمان واستخدام التكنولوجيا المرخصة، يمكن للمؤسسات الحكومية الحفاظ على سمعتها وضمان حماية بيانات المواطنين والمقيمين والمعلومات الحساسة الأخرى ذات الاهمية .

2.2 تصميم شبكة مقاومة:

تعزيز البنية التحتية لتكنولوجيا المعلومات تجاه التهديدات السيبرانية على الخدمات الرقمية الحكومية يعد أمرًا ضروريًا في ظل التطور المستمر للتهديدات السيبرانية وزيادة التعقيد والتطور في الهجمات الإلكترونية وتتطرق الدراسات والأبحاث إلى أهمية توفير حماية قوية للشبكات الحكومية الرقمية وتحديد التهديدات السيبرانية المحتملة التي يمكن أن تواجهها على سبيل المثال، هناك ممارسات في تصميم نظام متكامل للكشف المبكر عن الهجمات والرد عليها بسرعة لمنع وقوع أضرار جسيمة مما يشكل في أهمية التوازن بين الأمان والراحة والسهولة في الوصول إلى الخدمات الحكومية الرقمية ، حيث يجب أن تعتمد البنية التحتية على تقنيات الحماية المتقدمة والإجراءات الأمنية الصارمة دون المساس بالتنقل والوصول السلس للمستخدمين .

وتعزيز البنية التحتية لتكنولوجيا المعلومات ليس مجرد مسألة تقنية، بل يتطلب أيضًا التركيز على الجوانب الإدارية والتنظيمية والتعاون بين مختلف الجهات من خلال تبني منهاج العلمية في البحث والابتكار في مجال تعزيز البنية التحتية لتكنولوجيا المعلومات ومكافحة التهديدات السيبرانية عن طريق التعمق في الدراسات الخاصة لفهم طبيعة التهديدات السيبرانية وتحليل أنماط الهجمات والثغرات الأمنية الشائعة.

وتصميم شبكة مقاومة يهدف إلى بناء بنية تحتية قوية ومقاومة للهجمات السيبرانية من خلال بناء شبكة معمارية قوية تشمل جدران نارية قوية وتقنيات التشفير والتحقق من الهوية للكشف عن تهديدات محتملة ومنعها من الوصول إلى الشبكة الحكومية ويصاحبها تقييم واختبار أمن الشبكة بشكل دوري للكشف عن الثغرات الأمنية وتصحيحها قبل أن تتم استغلالها من المخترقين.

3.2 ضمان توفر الخدمة:

ضمان توفر الخدمة يشير إلى تصميم نظم احتياطية تضمن استمرارية الخدمة في حالة حدوث هجمات سيبرانية أو تعطل فني ويتطلب ذلك وجود نسخ احتياطية للبيانات وخطط لاستعادة الكوارث في حالة فقدان البيانات الحكومية أو تعطل الأنظمة الأساسية ويتم

إنشاء نسخ محدثة بشكل منتظم من قواعد البيانات والبرامج الرئيسية وتخزينها في مواقع بديلة عن بعد حتى في حال تعذر الوصول إلى المراكز الرئيسية كما يتم وضع إجراءات واضحة لاستعادة البيانات والأنظمة من النسخ الاحتياطية وإعادة الخدمات في أسرع وقت ممكن عند حدوث أي خلل أو طارئ وينبغي أيضًا تنفيذ استراتيجيات للتعامل مع حوادث التعطل الفني، مثل وجود فريق استجابة للطوارئ مجهز بالمهارات الفنية اللازمة وإجراءات واضحة لإدارة الأزمات وخاصه في الخدمات الحكومية بالدولة .

3. الحماية التقنية والتحديثات الأمنية:

الحماية التقنية والتحديثات الأمنية تلعب دورًا حاسمًا في ضمان أمن الخدمات الرقمية الحكومية وحمايتها من التهديدات السيبرانية ويتطلب تأمين الخدمات الحكومية من خلال تطوير استراتيجيات شاملة تتضمن عدة جوانب، وفيما يلي بعض النقاط الرئيسية التي يجب مراعاتها

1.3 تصميم وتنفيذ طبقات إضافية من الحماية: يتعين تطبيق نهج متعدد الطبقات للحماية، حيث يتم استخدام مجموعة متنوعة من التقنيات والأدوات لتوفير حماية شاملة ويمكن أن تشمل هذه الطبقات جدران الحماية، وأنظمة الكشف عن التسلل، وتقنيات التشفير، وأنظمة إدارة الهوية والوصول، والتوقيع الرقمي وغيرها وهي كالتالي:

- جدران الحماية (Firewalls): تعمل كحارس أول، حيث تفحص البيانات الداخلة والخارجة وتحجب تلك التي تشكل تهديدًا.
- أنظمة الكشف عن التسلل (SDI - smetsyS noitceteD noisurtnI): تراقب النشاط في الشبكة لتحديد محاولات الاختراق غير الشرعية.
- تقنيات التشفير: تضمن أن البيانات المنقولة أو المخزنة لا يمكن قراءتها من قبل أطراف غير مصرح لها.
- أنظمة إدارة الهوية والوصول (MAI - tnemeganaM sseccA dna ytitnedI): تضمن فقط للمستخدمين المصرح لهم الوصول إلى المعلومات الحساسة.
- التوقيع الرقمي: يستخدم للتحقق من صحة الوثائق الرقمية والتأكد من أنها لم تتغير أثناء النقل.

2.3 استخدام تقنيات الكشف المتقدمة للتصدي للتهديدات:

لتحسين القدرة على الكشف عن التهديدات والتصدي لها، يمكن الاستفادة من التقنيات الحديثة مثل الذكاء الاصطناعي والتعلم الآلي وهذه التقنيات وتساعد في

تحليل البيانات الضخمة والتعرف على الأنماط المشبوهة أو السلوكيات الغير معتادة التي قد تشير إلى هجوم أو تهديد أمني بالإضافة إلى ذلك، يعد الاستفادة من شبكات الاستشعار وأنظمة الاستجابة للحوادث من الأمور الضرورية لتوفير رؤية شاملة للبيئة الأمنية وتسريع الاستجابة للحوادث ويجب تطوير استراتيجيات تتضمن تحليلاً دقيقًا للمخاطر وتقييمًا مستمرًا للتهديدات السيبرانية

3.3 تحديثات أمان البرمجيات:

لتعزيز أمان الخدمات الرقمية الحكومية، يجب أن تتكامل الطبقات الأمنية لتشكيل حصن دفاعي محكم ويبدأ هذا بمبادئ تصميم النظام التي تأخذ بعين الاعتبار الأمان كأولوية منذ البداية وليس كإضافة لاحقة ويجب أن تشمل الإجراءات الوقائية تقنيات التحقق من الصلاحيات، والتحقق من صحة الإدخالات، وتقليل الامتيازات إلى الحد الأدنى الضروري لكل مستخدم

يعتبر التشفير القوي للبيانات المخزنة والمنقولة ضروريًا، بما في ذلك استخدام بروتوكولات شبكية حديثة مثل SLT لتأمين الاتصالات ويجب أن تشمل الأمان أيضًا التحقق المستمر من سلامة النظام للكشف عن أي تغييرات غير مصرح بها والاستجابة لها بسرعة.

4.3 تنفيذ سياسات لضمان التوافق مع متطلبات الأمان:

ينبغي وضع سياسات وإجراءات يتم اتباعها بدقة لضمان التوافق مع متطلبات الأمان القائمة ومنها:

- سياسات الاستخدام المقبول: تحديد كيفية استخدام الموارد التقنية بطريقة آمنة ومسؤولة.
- سياسات النسخ الاحتياطي والاسترداد: إنشاء وتطبيق سياسات للنسخ الاحتياطي واسترداد البيانات لتجنب فقدان المعلومات الحيوية.
- التحكم في الوصول: تقييد الوصول إلى المعلومات والموارد بناءً على الحاجة إلى المعرفة.
- التدقيق والمراقبة: مراقبة الأنظمة وتسجيل الأحداث لتحديد والتحقيق في الأنشطة المشبوهة.

5.3 تنظيم التحقيقات الأمنية: يجب تحديد إجراءات فعالة للتحقيق في حالات الاختراق والانتهاكات الأمنية ويتطلب ذلك وجود فرق متخصصة في التحقيق الرقمي لتحليل الأدلة الرقمية وتحديد المسؤوليات وتحديد مصادر الهجمات والتعامل معها بشكل فعال ويجب أيضًا توثيق وتحليل الحوادث الأمنية لتحسين الإجراءات المستقبلية وتعزيز الاستجابة للتهديدات.

بالإضافة إلى ذلك، تعتبر التعاون والتواصل مع مؤسسات أمن المعلومات والجهات المعنية الأخرى ضروريًا لتبادل المعلومات والخبرات وتعزيز القدرة على التصدي للتهديدات السيبرانية كما يجب أن تتبنى الحكومة أيضًا إطارًا قانونيًا وسياسيًا قويًا لتعزيز الحماية السيبرانية وتحقيق تنسيق فعال بين الجهات المعنية.

4. استخدام تقنيات كشف واستجابة للحوادث الأمنية:

تقنيات الكشف والاستجابة للحوادث الأمنية تعد مجالًا حيويًا ومتطورًا في مجال أمن المعلومات ويتطلب هذا المجال فهمًا عميقًا لأنماط الهجمات والتهديدات السيبرانية والتقنيات المتقدمة للكشف والتحليل ويتم تطبيق هذه التقنيات على الخدمات الحكومية الرقمية لحماية البيانات الحكومية الحساسة وضمان استمرارية العمليات الحكومية المهمة وبالتالي، تلعب هذه التقنيات دورًا حاسمًا في تعزيز أمان وثقة الجمهور في الخدمات الحكومية الرقمية في الدولة

1.4 تقنيات الكشف المتقدمة:

يتم الكشف عن أنماط غير طبيعية في حركة المعلومات من خلال استخدام تقنيات متقدمة للكشف عن أنماط غير طبيعية في حركة المعلومات داخل النظام الحكومي الرقمي، وذلك عن طريق مراقبة وتحليل سجلات النشاط وسلوك المستخدمين للكشف عن أنشطة مشبوهة أو غير معتادة وقد يتم استخدام تقنيات التعلم الآلي وتحليل البيانات الضخمة لتحديد أنماط غير طبيعية وإشارة إلى وجود تهديدات أمنية

ويعتبر أنظمة الكشف التلقائي للكشف المبكر عن تهديدات سيبراني من التقنيات المتقدمة في الكشف التلقائي عن تهديدات سيبرانية قبل حدوث أي ضرر كبير ويتم استخدام الذكاء الاصطناعي وتحليل السلوك للكشف عن أنماط الهجمات وتهديدات الأمان الجديدة ويمكن أن تتضمن هذه التقنيات استخدام أنظمة الكشف عن التسلل وأنظمة الاستشعار المتقدمة لرصد الأنشطة الغير مرغوب فيها على الشبكة.

2.4 إجراءات الاستجابة:

عند وضع خطط استجابة فعّالة للتعامل مع حالات الطوارئ الأمنية يتم وضع خطط استجابة تحتوي على إجراءات واضحة ومحددة للتعامل مع حالات الطوارئ الأمني وقد تشمل هذه الخطط إجراءات لإبطاء واحتواء التهديد وتقييم الأضرار واستعادة النظام الحكومي الرقمي بأسرع وقت ممكن ويتخلل هذا الاجراء تبني مناهج تدريب الفرق على تنفيذ إجراءات الاستجابة بشكل سريع وفعّاله مع مراعاة الاهتمام في الجانب التوعوي بالتهديدات السيبرانية المحتملة مع الاستمرار في إجراء تمارين ومحاكاة لحالات الطوارئ

لتقييم استعداد الفرق وتحسين استجابتها عند الاحداث الامنية المستقبلية .

3.4 تحليل الحوادث:

إجراء تحليل شامل للحوادث الأمنية لفهم الطبيعة والمصدر من خلال التحليل الشامل للحوادث الأمنية التي تحدث على الخدمات الحكومية الرقمية وقد يشمل ذلك تحليل الهجمات المنفذة وتحديد أسباب الفشل في الأمان وتحديد المصادر المحتملة للتهديدات ويمكن استخدام تقنيات التحليل الرقمي وتحليل السجلات والبيانات لفهم الأنماط والسلوكيات المشتبه بها وتحديد النقاط الضعيفة في الانظمة الحكومية.

ولاحظت وجود وفرة في التقارير التحليلية والتي توجه لإجراء التحسينات في استراتيجيات الكشف والاستجابة وتتضمن هذه التقارير تقييمًا للأضرار والتأثيرات وتوجيهات لتعزيز استراتيجيات الكشف والاستجابة ويمكن استخدام هذه التقارير لاتخاذ تحسينات في السياسات والإجراءات الأمنية ولتحسين الوعي بالأمان وتعزيز القدرة على التصدي للتهديدات السيبرانية في المستقبل.

5. التعاون المؤسساتي في مجال الأمن السيبراني:

التعاون المؤسساتي في مجال الأمان السيبراني يلعب دورًا حاسمًا في حماية الخدمات الحكومية الرقمية من التهديدات السيبرانية المتزايدة من خلال تنسيق الجهود بين الجهات الحكومية والمؤسسات المعنية، ويمكن تحقيق مستوى أعلى من الحماية والامن السيبراني.

أحد جوانب التعاون المؤسساتي هو التنسيق مع الجهات الحكومية ذات الصلة يتم تعزيز التعاون مع هذه الجهات من أجل تبادل المعلومات المتعلقة بالتهديدات السيبرانية والتحديات الأمنية الأخرى ويمكن أن يشمل ذلك مشاركة المعلومات الهامة حول الهجمات السيبرانية، والتحذيرات المبكرة، والتوجيهات الأمنية عن طريق التنسيق مع الجهات الحكومية، يمكن تعزيز القدرة على استجابة سريعة وفعالة للتهديدات السيبرانية بالإضافة إلى ذلك، لوحظ هناك تحديد مهم في الأدوار والمسؤوليات لكل جهة مشاركة في تعزيز الأمن السيبراني ويرافقه توزيع واضح للمسؤوليات بين الجهات المشاركة، بما في ذلك الجهات الحكومية والمؤسسات الخاصة والأكاديمية مما قد يوفر آليات فعالة لتنظيم وتنسيق هذه الأدوار والمسؤوليات، بحيث يتم تحقيق أعلى مستويات الفعالية في مكافحة التهديدات السيبرانية .

تعزيز التعاون مطلب استراتيجي مهم يتخلله تنفيذ برامج تدريب مشتركة وورش عمل لتعزيز المعرفة والمهارات في مجال الأمان السيبراني مع الجهات المختصة ويمكن للجهات

المشاركة أن تستفيد من تبادل المعرفة والخبرات، وتطوير استراتيجيات وتقنيات جديدة لمكافحة التهديدات السيبرانية على المدى البعيد مع عدم الاغفال عن تعزيز الوعي الأمني وتطوير مهارات الاستجابة للحوادث السيبرانية للعاملين والمتعاملين.

ويعد التعاون المؤسساتي مع التهديدات السيبرانية التي تواجه الخدمات الحكومية الرقمية مثل الاختراقات الهجينة، وهجمات الفدية، والتجسس السيبراني، وتعطيل الخدمات الحكومية والخ من هذه التهديدات مع الجهات الحكومية والأكاديمية دور بارز وحلقة وصل مهمة وخطيرة يمكنها في أن تساهم في تحديد النقاط الضعيفة وتطوير استراتيجيات الدفاع الفعالة في المؤسسات بالدولة

6.مراجعة وتقييم الاستراتيجية الوقائية:

تقوم الحكومات بتنفيذ استراتيجيات وقائية لحماية خدماتها الحكومية الرقمية من التهديدات السيبرانية ومن أجل ضمان فعالية هذه الاستراتيجيات، تقوم هذه الجهات المعنية إجراء تقييم دوري لأدائها ويشمل ذلك تحليل النتائج المتحققة وتحديد مدى تحقيق الأهداف المحددة في الاستراتيجية ويمكن استخدام مجموعة من المقاييس والمؤشرات لقياس تأثير الاستراتيجية على الحد من التهديدات السيبرانية وتعزيز الأمان الرقمي للخدمات الحكومية

يعد تحليل الحوادث الأمنية السابقة جزءًا هامًا من عملية تقييم الاستراتيجية الوقائية ويتم من خلال فحص الحوادث السابقة وتحليلها، يمكن للحكومات تحديد الثغرات والأخطاء التي أدت إلى حدوث هذه الحوادث، وبالتالي تجنب تكرارها في المستقبل ويمكن أيضًا استخدام النتائج المستخلصة من التقييم للاستفادة من التجارب السابقة، وتطوير وتحسين الأداء الأمني للخدمات الحكومية الرقمية

بناءً على الدروس المستفادة من تقييم الأداء وتحليل الحوادث السابقة، يجب على الحكومات تحديث استراتيجياتها الوقائي ويمكن أن يشمل ذلك تحديث السياسات والإجراءات الأمنية، وتحسين التدريب والتوعية الأمنية للموظفين، وتعزيز التعاون مع القطاع الخاص والمؤسسات الأخرى ذات الصلة وكما ينبغي أيضًا استكشاف وتبني أحدث التقنيات والأساليب الأمنية المتاحة للتصدي للتهديدات السيبرانية المتطورة ويتطلب ذلك متابعة التطورات التكنولوجية والأمنية، وتقييم مدى توافر الحلول الجديدة وفعاليتها في سياق الأمن الحكومي.

بالاستفادة من تقييم دوري للأداء وتحليل الحوادث السابقة، وتحديث الاستراتيجية الوقائية واستكشاف وتبني التقنيات والأساليب الأمنية الحديثة، يمكن للحكومات تعزيز

قدرتها على حماية الخدمات الحكومية الرقمية من التهديدات السيبرانية علاوة على ذلك، التركيز في تعزيز التوعية الأمنية للموظفين والمستخدمين وتعزيز التعاون مع القطاع الخاص والشركاء الأمنيين الآخرين للتصدي للتهديدات السيبرانية بشكل فعال، ويمكن القول أن تكون الاستراتيجية الوقائية للحكومة شاملة ومتكاملة، وتغطي جميع جوانب الأمن السيبراني بما في ذلك الجوانب التقنية والسياسية والقانونية والتنظيمية وتتماشى الاستراتيجية مع المعايير والممارسات الأمنية العالمية، وتأخذ بعين الاعتبار التهديدات الحالية والناشئة في مجال السيبرانية على مستوى العالم .

وتأخذ الحكومات الجدية في تعزيز قدراتها الدفاعية والاستجابة للتهديدات السيبرانية المحتملة و لديها آليات لرصد واكتشاف التهديدات والاعتداءات السيبرانية، وللتعامل معها بشكل فعال وسريع ولديها امكانيات وقدرات في التعافي من الهجمات السيبرانية، بما في ذلك إجراءات النسخ الاحتياطي واستعادة البيانات، وإعادة تأهيل الأنظمة المتأثرة حيث لاحظت عندما تكون هناك استراتيجية في الأمن السيبراني للخدمات الحكومية الرقمية محدثه عبر السنوات ومستدامة وتجرى عليها عمليات التطوير بشكل مستمر وتتكيف مع التغيرات التكنولوجية والتهديدات السيبرانية المتطورة مع تبني الأساليب والتقنيات الأمنية الحديثة والتعاون المستمر مع الجهات المعنية يظهر الجانب المميز الامني في المؤسسات و تشكل أمرًا مهما وحاسمًا لتعزيز الأمن السيبراني للخدمات الحكومية وحماية المعلومات والبيانات الحساسة في دولة الامارات.

7. إنشاء قاعدة بيانات مركزية لمعلومات الحوادث:

يعد إنشاء قاعدة بيانات مركزية لمعلومات الحوادث ادوات مهمة وتعد ركيزة أساسية لتعزيز كفاءة الخدمات الحكومية الرقمية وهدفها هو جمع البيانات المتعلقة بالحوادث من مصادر متعددة وتوحيدها في مستودع مركزي يسهل الوصول إليه وتحليله وتحتوي على بعض العناصر والمكونات الرئيسية لتصميم وإدارة هذه القاعدة بشكل فعال ومستدام وتشمل عملية إنشاء قاعدة بيانات مركزية لمعلومات الحوادث عدة خطوات بما في ذلك الجداول والعلاقات بينها ويتم تحديد الحقول والمتغيرات المختلفة التي يتم تخزينها في القاعدة بيانات، مثل تفاصيل الحادث والتوقيت والموقع والأطراف المعنية وغيرها ويتم تصميم نظام قواعد البيانات لتوفير أداء عالي وكفاءة في استرجاع المعلومات وعند تصميم البنية التحتية لقاعدة البيانات يتم نمذجة البيانات من خلال تحديد الكيانات والعلاقات الأساسية التي ستشكل جدول البيانات، مثل الحوادث، الضحايا، الجناة، الشهود، وأنواع الحوادث والخ من الحقول المهمة في الامن السيبراني وينشى على ثره المخطط العلاقي ويوضح به كيفية ترابط هذه الجداول والعلاقات بينها (مثل جداول الارتباط

للعلاقات العديدة إلى العديد) ، ويوجد تحديد مجموعة من الحقول مثل تاريخ الحادث، موقعه، والتفاصيل المتعلقة بالأضرار والخسائر وتربط مع مؤشرات الأداء من خلال إدراج مؤشرات للأداء لتسهيل تتبع وتحليل البيانات بشكل دوري

تعتبر الحكومات مصدرًا هامًا للمعلومات الحساسة والسرية، ويتم توفير إجراءات أمان قوية لحماية هذه البيانات ويتضمن ذلك تنفيذ تقنيات التشفير المناسبة لضمان سرية البيانات، وتطبيق آليات وسياسات الوصول المحددة للتحكم في من يمكنه الوصول إلى المعلومات، وتنفيذ تدابير الحماية الفعالة لمنع الاختراق والاعتداء على النظام ويعد تأمين البيانات مثل التشفير اداء قوية للبيانات تستخدم في أثناء النقل والتخزين لحماية المعلومات الحساسة ويمكن لإدارة الهوية والوصول في المساهمة لتحديد سياسات واضحة لمن يمكنه الوصول إلى البيانات ونوع الوصول المتاح عبر جميع القطاعات الخدمية ولأغراض الجودة يتم التدقيق والمراقبة عن طريق إنشاء سجلات تدقيق لتتبع الوصول إلى البيانات والتغييرات التي تطرأ عليها ويعد النسخ الاحتياطي والاسترداد من الاسلحة القوية الصامدة امام التهديدات من اجل ضمان استمرارية الأعمال وعدم فقدان البيانات في الخدمات الرقمية الحكومية

وفي عصر الذكاء الاصطناعي تقوم الشركات الرائدة في تخزين المعلومات في قاعدة البيانات المركزية وتستخدم أساليب تحليل البيانات للاستفادة القصوى من هذه المعلومات يتضمن ايضا استخدام تقنيات التنقيب في البيانات وتحليل البيانات الضخمة لاستخلاص الأنماط والاتجاهات المفيدة وتحليل البيانات واكتشاف العلاقات والتنبؤ بتطور الحوادث المستقبلية

المبحث الثاني

توفير التوعية السيبرانية المستمرة والتطوير المستمر للموظفين لتحسين مستوى الأمن السيبراني

- **أهمية التوعية السيبرانية للموظفين :**

تعتبر التوعية السيبرانية للموظفين أمرًا حيويًا في تعزيز الأمن السيبراني والحماية ضد التهديدات السيبرانية حيث يزيد توفير التوعية المستمرة للموظفين من وعيهم بأهمية في الأمن السيبراني والتهديدات المحتملة ويتم تزويدهم بالمعرفة والفهم الضروريين للتصرف بشكل آمن واتخاذ إجراءات سليمة في التعامل مع المعلومات الحساسة والإبلاغ عن أي اختراق محتمل في الادارة.

وتساهم التوعية السيبرانية في حماية البيانات والمعلومات الحساسة من التهديدات الداخلية من خلال زيادة الوعي بوجود التهديدات الداخلية وتحديد السلوكيات غير المشروعة أو المشبوهة، ويمكن اتخاذ التدابير اللازمة للوقاية من الاختراقات الداخلية والحفاظ على سلامة النظام والبيانات في القطاعات الحكومية.

وتساعد التوعية السيبرانية في مكافحة الهجمات الاجتماعية ويشمل ذلك الهجمات التي تستهدف استغلال ضعف الموظفين وخداعهم للوصول إلى المعلومات الحساسة ويمكن للتوعية السيبرانية المستمرة توعية الموظفين بمثل هذه الهجمات وتعزيز قدرتهم على التعرف عليها وتجنب الوقوع في الفخ السيبراني.

ويعد توفير التوعية السيبرانية المستمرة للموظفين أمرًا حاسمًا في تعزيز الوعي والمسؤولية والتصرف السليم في مجال الأمن السيبراني ويمكن لهذا الوعي أن يقلل من فرص الوقوع في الفخ والاختراقات السيبرانية، ويساهم في حماية البيانات الحساسة والمصالح الوطنية وبالتالي، ويستدعى من المؤسسات الحكومية الاستثمار الفعال في برامج التوعية السيبرانية وتوفير التدريب والموارد اللازمة لتطوير قدرات الموظفين في هذا المجال.

- **دور الموظفين في تحسين الأمن السيبراني:**

يلعب الموظفون دورًا حاسمًا في تحسين الأمن السيبراني للخدمات الحكومية الرقمية من خلال وعيهم ومشاركتهم الفعالة في مبادرات الأمن السيبراني، يمكن تعزيز الوعي والمسؤولية الفردية وتحسين الحماية ضد التهديدات السيبرانية حيث بإمكان الموظفين أن يساهموا في تحسين الأمن السيبراني من خلال تبني الممارسات الأمنية الصحيحة على سبيل المثال، يجب أن يكونوا حذرين في استخدام كلمات المرور القوية وتحديثها بشكل منتظم كما ينبغي عليهم عدم مشاركة معلومات الدخول الشخصية مع الآخرين وتجنب فتح رسائل البريد الإلكتروني المشبوهة أو المرفقات غير المعروفة.

وهناك من الموظفين على استعداد للتبليغ عن الاختراقات المحتملة عند ملاحظة أي نشاط غريب أو مشتبه به، عن طريق الإبلاغ عنه فورًا إلى فريق الأمن السيبراني المختص وهذا التصرف يمكن أن يساهم في اكتشاف التهديدات المبكرة واتخاذ التدابير اللازمة للتصدي لها قبل أن تتسبب في أضرار كبيرة على المؤسسة الحكومية.

ولوحظ وجود عدد من الموظفين ملتزمون بالمشاركة في برامج التدريب وورش العمل المتعلقة بالأمن السيبراني ويمكن لهذه الفعاليات تعزيز الوعي وتعليم الموظفين حول أحدث التهديدات السيبرانية وكيفية التصدي لها بالإضافة إلى ذلك، يمكن للموظفين

تطوير مهاراتهم الفردية في مجال الأمن السيبراني وتطبيقها في عملهم اليومي وبالتالي يلعب الموظفون دورًا حيويًا في تحسين مستوى الأمن السيبراني للخدمات الحكومية الرقمية من خلال تبني الممارسات الأمنية الصحيحة، والتبليغ عن الاختراقات المحتملة، والمشاركة في برامج التدريب وورش العمل، وتعزيز الوعي والمسؤولية الفردية وتحقيق مستوى أعلى من الأمن السيبراني في المؤسسة .

ان تحقيق التوعية المستمرة للموظفين يعزز من الأمن السيبراني بشكل ملموس، ويترتب عليه آثار إيجابية متعددة حيث تتيح التوعية المستمرة في تقليل معدل حدوث الاختراقات من خلال زيادة الوعي والفهم لدى الموظفين، ويمكن تقليل فرص الوقوع في فخاخ الهجمات السيبرانية، مما يسهم في حد من معدل حدوث الاختراقات ويساهم التوعية المستمرة في تعزيز الاستجابة الفعالة علما الموظفون الذين يتسلحون بالمعرفة يستطيعون الاستجابة بفعالية في حالة اكتشاف أو توقع حدوث تهديد سيبراني، مما يقلل من التأثيرات السلبية ويعزز قدرة الرد الفوري

ويعكس تأثير التوعية المستمرة في تحسين سلوكيات الأمن الموظفون الذين يفهمون أهمية الأمان السيبراني يتبنون ممارسات أمنية أفضل في استخدام التكنولوجيا وحماية المعلومات الحساسة ويُعزز التوجيه المستمر في ثقافة الأمن داخل المؤسسة حيث يشجع الموظفين على التكامل بشكل أفضل في جهود حماية المعلومات ويساهم في تحقيق بيئة داخلية تُشجع على الوعي والمسؤولية في مجال الأمن السيبراني.

- **التحديات الرئيسية في توفير التوعية السيبرانية المستمرة:**

توفير التوعية السيبرانية يشكل تحديًا رئيسيًا في مجال الأمن السيبراني وتظهر بعض التحديات الرئيسية التي تواجه عمليات التوعية كالتالي:

أولًا: تتغير التهديدات السيبرانية بسرعة وتتطور باستمرار مما يصعب فرق التوعية السيبرانية مواكبة هذه التغيرات بشكل فوري وتحديث المحتوى والمواد التوعوية بشكل مستمر وقد يكون من الصعب للغاية توفير التحديثات المستمرة وتطوير مواد توعية فعالة للتعامل مع التهديدات الجديدة

ثانيًا: الوعي السيبراني يعتمد بشكل كبير على تفاعل المستخدمين والموظفين وتبنيهم للممارسات الأمنية الصحيحة وقد يكون من التحديات تشجيع المستخدمين على اتخاذ التدابير الأمنية والامتناع عن السلوكيات الخطرة على الإنترنت والشبكة الداخلية في العمل وقد يواجه المتعاملون صعوبة في فهم التهديدات السيبرانية المحتملة وتطبيق الإجراءات الوقائية المناسبة لهم

ثالثًا: قد يكون التوعية السيبرانية مهمة ضخمة للمؤسسات ذات المقياس الكبير

لتنظيمها في الشركات والحكومات التي لديها العديد من الموظفين والمستخدمين، ومن الممكن أن تكون هناك صعوبة في توفير التدريب والتوعية الفعالة للجميع وقد يكون من التحديات تنظيم برامج التوعية الشاملة وتخصيص الموارد المالية والبشرية اللازمة لتحقيق التغطية الشاملة

- **تحليل التحديات التي تواجه عمليات التوعية السيبرانية:** عند تحليل التحديات التي تواجه عمليات التوعية السيبرانية بالمؤسسات الحكومية في الدولة، وهناك مراعاة لعدة عوامل رئيسية:

أولًا: قد يكون التفاهم الضعيف للمستخدمين حول التهديدات السيبرانية وأهميتها أحد التحديات الرئيسية ويعتبر البعض أمورًا مثل تحديث البرامج أو استخدام كلمات مرور قوية أمورًا مزعجة وغير ضرورية وقد يكون من الصعب إقناع المستخدمين بأنهم الجزء الأساسي في سلسلة الحماية وأن تصرفاتهم يمكن أن تؤثر على الأمن السيبراني.

ثانيًا: تعتبر قيود الموارد المالية والبشرية عاملًا مهمًا يؤثر على عمليات التوعية وقد يكون من التحديات توفير الميزانية الكافية لتطوير وتنفيذ برامج التوعية السيبرانية الشاملة بالإضافة إلى ذلك، تتطلب التوعية السيبرانية فرق متخصصة ومدربة لتنفيذها وتقديم المشورة والدعم المستمر للمستخدمين وقد يكون من الصعب توفير هذه الموارد البشرية اللازمة في بعض الأحيان وفي كل القطاعات الحكومية.

ثالثًا: الفهم المتغير للتهديدات السيبرانية والتكنولوجيا المتقدمة يشكل تحديًا حيث التهديدات السيبرانية متطورة باستمرار وتستخدم تقنيات جديدة للاختراق ويكون من التحديات توفير التدريب والمواد التوعوية التي تواكب هذا التطور وتعليم المستخدمين كيفية التعامل مع التهديدات الحديثة المستمرة.

رابعًا: يعتبر عدم التزام القيادة والدعم الكافي لعمليات التوعية أحد التحديات الشائعة فإذا لم تعتبر القيادة الأمن السيبراني وعمليات التوعية جزءًا أساسيًا من الاستراتيجية العامة للمؤسسة الحكومية، فقد يؤدي ذلك إلى تقليل الأهمية المعطاة للتوعية والتقليل من جودتها وتأثيرها مما يستوجب من القيادة الادراك بأهمية التوعية وتعززها من خلال تخصيص الموارد والتأكيد على أهميتها في جميع أنحاء المؤسسة الحكومية.

- **أساليب توفير التوعية السيبرانية:** توفر التوعية السيبرانية في المؤسسات الحكومية يمكن تحقيقها من خلال مجموعة متنوعة من الأساليب والنماذج وبرامج التوعية السيبرانية:

الحملات التوعوية عبر البريد الإلكتروني وانظمة التراسل الداخلية: تُرسل حزمة من رسائل البريد إلكتروني لتوعوية وتحذير الموظفين في المؤسسات الحكومية وتتضمن هذه الرسائل نصائح وإرشادات للتصرف الآمن على الإنترنت والشبكات الداخلية في العمل وكيفية التعرف على رسائل البريد الإلكتروني المشبوهة والصفحات الخبيثة.

- يمكن للذكاء الاصطناعي أن يساعد في تعريف المستخدمين على أنماط البريد الإلكتروني المشبوه والاحتيال الإلكتروني من خلال تحليل البيانات السابقة للبريد الإلكتروني وتحديد العلامات التي تشير إلى البريد الإلكتروني المشبوه، مثل روابط غير معروفة أو طلبات مالية غير مبررة ويمكن توفير تدريب متكرر للمستخدمين للتعرف على هذه العلامات وتجنب الوقوع ضحية للهجمات السيبرانية

- **البرامج التعليمية والمنصات التطبيقية:** تقدم منصات وتطبيقات التعلم عبر الإنترنت والشبكة الداخلية للموظفين دورات ودروسًا توعوية حول الأمن السيبراني والتصرف الآمن على الإنترنت والشبكة الداخلية في العمل حيث يتم تعليم المستخدمين حول التهديدات السيبرانية المشتركة والأساليب الفعالة لحماية البيانات الشخصية والمعلومات الحساسة.

- **ورش العمل السيبراني والندوات:** تُعقد سلسة من ورش العمل والندوات المتخصصة حول الأمن السيبراني والتوعية ويتم توفير محاضرات وعروض توضيحية تفاعلية للمشاركين لتعزيز الوعي وتقديم النصائح العملية لحماية الأنظمة والبيانات من قبل المختصين والخبراء في هذا المجال

- **توفير المواد التوعوية:** يتم إنتاج وتوزيع مواد توعوية مثل بروشورات وملصقات وملفات FDP التي تحتوي على معلومات هامة حول الأمن السيبراني والتدابير الوقائية ويتم توزيعها في المكاتب وكاونترات الخدمة وجميع مرافق المباني الحكومية لتعميم الوعي حول التهديدات السيبرانية.

- **محاكاة الهجمات والتدريب:** توجد مجالات عديدة في استخدام الذكاء الاصطناعي لإنشاء بيئة محاكاة للهجمات السيبرانية ويمكن تنفيذ هجمات افتراضية ومحاولة اختراق النظام بأمن لتوعية المستخدمين بأنواع الهجمات وتأثيرها المحتمل

توجيه النصائح والتوصيات: بالإمكان استخدام تقنيات التعلم الآلي في تحليل النشاطات الحالية للمستخدمين وتوجيههم بنصائح وتوصيات محددة لتحسين الأمن السيبراني ويمكن أن تشمل هذه التوصيات استخدام كلمات مرور قوية، وتحديث البرامج والتطبيقات بانتظام، وتجنب الفتح المشبوه للمرفقات أو الروابط غير المعروفة ولهذه النصائح الفردية

والمخصصة يمكن أن تعزز الوعي السيبراني للمستخدمين.

تحليل مدى فعالية أساليب التوعية السيبرانية: لتحليل فعالية أساليب توفير التوعية السيبرانية يمكن أن يساعدنا في تحديد ما إذا كانت تلك الأساليب فعالة النقاط التالية:

التفاعلية: تعتبر الأساليب التوعوية التفاعلية أكثر فعالية عادةً على سبيل المثال، ورش العمل والندوات تسمح للمشاركين بطرح الأسئلة ومناقشة التحديات السيبرانية الخاصة بهم، مما يعزز التعلم والفهم ويزرع في عقولهم المعلومات ويزيدهم ادراكها حولها

- **الشمولية:** يمكن ان تكون الأساليب شمولية لجميع الفئات المستهدفة، سواء كانوا موظفين في المؤسسات، مدراء الوحدات التنظيمية، أو أفراد في المجتمع الذين يستخدمون الخدمات الرقمية الحكومية وعادة تكون الرسائل والمواد التوعوية مفهومة وملائمة للجميع، بغض النظر عن مستوى المعرفة السابقة في مجال الأمن السيبراني.
- **التكرار:** يعتبر توفير التوعية المستمرة والمتكررة أمرًا هامًا من خلال تكرار توجيهات الأمن والنصائح بشكل منتظم لتعزيز الوعي والتذكير بأهمية الاستمرار في ممارسات الأمان السيبراني بين مختلف شرائح الموظفين والمتعاملين في الدولة.
- **تقييم الفعالية:** يجب تقييم فعالية هذه الأساليب باستمرار من خلال تتبع المشاركة وتقييم تغيير سلوك المستخدمين بعد المشاركة في برامج التوعية ويمكن استخدام استبيانات واختبارات لقياس المعرفة والفهم وتقييم التغير في سلوك المستخدمين فيما يتعلق بالأمن السيبراني.

دور التدريب وورش العمل في تطوير مهارات الموظفين: قامت العديد من المؤسسات الحكومية في اعداد التدريب المناسب وورش العمل الملائمة في تطوير مهارات الموظفين في مجال الأمن السيبراني عن طريق توفير فرص التدريب التخصصية المستمرة، وتعزيز الوعي والمعرفة حول أحدث التهديدات السيبرانية والأدوات والتقنيات اللازمة للتصدي لها من خلال النقاط الاسترشادية التالية:

- **توفير المعرفة والمهارات:** يعد توفير التدريب المتخصص في مجالات مثل أمن الشبكات، واختبار الاختراق، وإدارة الحوادث السيبرانية من التقنيات المهمة ويتيح للموظفين فرصة لاكتساب المعرفة اللازمة لفهم التهديدات السيبرانية والتقنيات المستخدمة في الدفاع عن الشبكات ويمكن تنظيم ورش عمل تفاعلية تسمح للمشاركين بتجربة الأدوات والتقنيات الجديدة في بيئة تعليمية ويمكنهم التدرب على

استخدام أدوات الحماية ومكافحة الاختراق والتحقق من الثغرات الأمنية.

- **تطوير الوعي وتغيير السلوك:** تستعين المؤسسات الحكومية في ورش العمل والتدريب لزيادة الوعي بأهمية الأمن السيبراني والتأكيد على دور كل فرد من المجتمع والموظفين في حماية المعلومات والبيانات المهمة للمؤسسة الحكومية ويمكن استعراض سيناريوهات واقعية للهجمات السيبرانية وتأثيرها على العملية العادية للمؤسسة وهذا يساعد في توضيح التهديدات المحتملة ويشجع الموظفين على اتخاذ التدابير الوقائية اللازمة وعلى ثر ذلك ، يمكن تعزيز السلوك الآمن من خلال تعزيز ممارسات مثل استخدام كلمات مرور قوية وتحديث البرامج وعدم مشاركة المعلومات الحساسة عبر البريد الإلكتروني غير المشفر، وغيرها من الإجراءات الأمنية المهمة.
- **تنمية الخبرة والتخصص:** تفضل المؤسسات الحكومية منهجية التطوير المستمر، من خلال تمكين الموظفين من تنمية خبراتهم في مجال الأمن السيبراني وتحسين تخصصاتهم عن طريق التعمق في تعلم أحدث الأدوات والتقنيات والمتطلبات القانونية والتنظيمية في مجال الأمن السيبراني ويمكن للموظفين المدربون بشكل مستمر يمكن أن يعدوا خبراء سيبرانيين داخل المؤسسة الحكومية في مجال الأمن السيبراني ويمكنهم تبادل المعرفة والخبرات بين جميع الموظفين.

قياس تأثير التطوير المستمر على مستوى الأمن السيبراني:

- **تقييم المعرفة والمهارات:** تقوم المؤسسات الحكومية في إجراء اختبارات للتأكد من فهم الموظفين للمفاهيم الأساسية في مجال الأمن السيبراني وقدرتهم على تطبيقها في الأعمال العملية، ويمكن استخدام نتائج هذه الاختبارات لتحديد المجالات التي تحتاج إلى تحسين وتوجيه الجهود التدريبية بناءً على ذلك.
- **تحليل السلوك والممارسات:** تهتم المؤسسات الحكومية في مراقبة سلوك الموظفين وممارساتهم فيما يتعلق بالأمن السيبراني، مثل توثيق استخدام كلمات المرور القوية والالتزام بسياسات الأمن حيث يمكن استخدام هذه المعلومات لتقييم التحسينات وتحديد المجالات التي تحتاج إلى تعزيز لتقوية الموظفين والمتعاملين وتسليحهم ضد التهديدات السيبرانية المختلفة.
- **قياس معدل الحوادث الأمنية:** تعتمد المؤسسات الحكومية على قياس عدد الحوادث الأمنية والاختراقات التي يتعرض لها النظام السيبراني للمؤسسة بعد فترة التطوير المستمرة حيث إذا تم تحقيق تحسن في هذا المجال فإن ذلك قد يشير إلى

نجاح الجهود التدريبية وتطبيق الممارسات الأمنية.

- **تقييم رضا الموظفين:** تجري المؤسسات الحكومية استطلاعات رضا الموظفين لقياس مدى رضاهم عن برامج التطوير المستمر في مجال الأمن السيبراني وبذلك توفر التغذية الراجعة لإرشادات قيمة حول التحسينات المحتملة واحتياجات التدريب المستقبلية حول الامن السيبراني.
- **تقييم الأداء ومراقبة التطور:** تقييم الأداء ومراقبة التطور في مجال التوعية السيبرانية وتطويرها أمران حيويان لتحسين مستوى الأمان السيبراني في المؤسسات الحكومية وفي هذا السياق، لوحظ وجود عدة طرق مستخدمة لتقييم تأثير التوعية والتطوير: -
- **تقييم تأثير التوعية والتطوير:** تقييم تأثير التوعية والتطوير يتطلب استخدام أدوات وطرق فعالة لقياس التغير في سلوك ومعرفة الموظفين بشأن الأمن السيبراني ومن بين الطرق الشائعة المستخدمة في معظم القطاعات الحكومية:

◊ **استبيانات التوعية:** تقوم الجهات الحكومية في إعداد استبيانات تقييمية لقياس مستوى الوعي والمعرفة لدى الموظفين في مجال السيبرانية وتشمل هذه الاستبيانات أسئلة حول الممارسات الأمنية، والتهديدات السيبرانية، والسلوك الآمن على الإنترنت واثناء انجاز الخدمات الحكومية وتقوم بتحليل النتائج لتوفير رؤية واضحة حول النقاط القوية والضعف ويساعد في توجيه جهود التطوير المستقبلية.

◊ **اختبار الوعي:** تسعى الجهات الحكومية بين الحين والاخر الى إجراء اختبارات لقياس مستوى الوعي الفعلي والتصرفات الأمنية للموظفين في سيناريوهات واقعية من خلال تقنيات عديدة ومنها استخدام اختبارات الاختراق (gnitseT noitarteneP) وهجمات الصيد الاحتيالية (skcattA gnihsihP)) كأدوات لتقييم استجابة الموظفين للتهديدات السيبرانية والتصرفات الأمنية عند حدوث تهديدات حقيقية على الخدمات الحكومية.

◊ **مراجعات الأداء:** لوحظ وجود ممارسات حكومية لمراجعات الأداء الدورية والتي تشمل تقييم أداء الموظفين في مجال الأمن السيبراني وتحتوي على تحليل مدى الامتثال للسياسات والإجراءات الأمنية وتقدير قدرة الموظفين على التعامل مع التهديدات السيبرانية واتخاذ الإجراءات الوقائية.

- **آليات فعالة لمراقبة التقدم:** لأغراض استمرارية التطوير ومراقبة التقدم في تطوير التوعية السيبرانية وتحسين مستوى الأمن السيبراني، تعتمد المؤسسات الحكومية عدد معين من المبادرات ومنهاج العمل في مراقبة التقدم الحاصل وفعاليتها على

البيئة المؤسسية ومنها:

- **المتابعة المستمرة:** يتم فيها توفير متابعة مستمرة لتحليل التقدم في مجال التوعية والتطوير عن طريق الفرق الفنية المتخصصة واللجان المعتمدة وتلجأ الى استخدام أنظمة إدارة التعلم (smetsyS tnemeganaM gninraeL) لتتبع تقدم مستوى الموظفين في دورات التوعية السيبرانية وتحديثاتها.
- **تقييم التغطية:** ينبغي أن يتم تقييم درجة تغطية برامج التوعية والتطوير في المؤسسة ويمكن مراجعة القائمة بالموظفين الذين شاركوا في البرامج وتحليل النسبة المئوية للمشاركة كما يمكن لزيادة التغطية تأثير إيجابي على مستوى الأمان السيبراني في المؤسسة.
- **رصد الحوادث الأمنية:** تهتم القطاعات الحيوية في رصد الحوادث الأمنية والتهديدات المحتملة بشكل دوري عن طريق استخدام أنظمة رصد الأمان (gnirotinoM ytiruceS smetsyS) وتحليل السجلات (sisylanA goL) لتتبع الأنشطة غير المرغوب فيها والاعتداءات السيبرانية المحتملة ويساعد ذلك في تحديد الثغرات واتخاذ التدابير الوقائية المناسبة بالمؤسسة.
- **تقييم التدريبات والمواد التعليمية:** من المبادئ المهمة في قطاعات التطوير والتدريب تقييم فعالية التدريبات والمواد التعليمية المستخدمة في برامج التوعية والتطوير من خلال استخدام تقييمات ما قبل وما بعد التدريب لقياس تحسن المعرفة والمهارات الأمنية للموظفين وتشمل أيضًا الاعتماد على تقييمات المشاركين وملاحظاتهم لتحديد نواحي التحسين وتعزيز جودة التدريبات المقدمة إليهم.
- **المقارنة بالمعايير القياسية:** تسعى ادارة الجودة في القطاعات الحكومية في تبني المعايير القياسية والممارسات الأفضل في مجال التوعية من خلال مقارنة ادائها مع جهات ريادية في مجال الامن السيبراني والتي تتيح هذه المقارنة للمؤسسات في تحديد الفجوات والنقاط التي يجب تحسينها و تشمل المعايير القياسية عدة مجالات مهمة مثل سياسات الأمن، وإجراءات الأمن، وإدارة التهديدات، وقواعد السلوك الأمني، واستجابة الطوارئ السيبرانية، وتدريب الموظفين، وحماية البيانات، والتحقق من الهوية، وغيرها من المعايير المهمة في مجال الامن السيبراني .

- **دراسة حالة في أفضل الممارسات في مجال الامن السيبراني:** بولندا تعد دراسة حالات الدول الرائدة في مجال الأمن السيبراني ذات أهمية بالغة لاستقطاب أفضل

الممارسات وتوظيفها في تعزيز مستويات الحماية الوطنية وقد تم اختيار دولة (بولندا) كدراسة حالة نظراً لتفوقها في المؤشرات العالمية ذات الصلة:

حيث تعتبر بولندا دولة متقدمة في مجال الأمن السيبراني حيث يبلغ عدد سكانها 4.83 مليون نسمة، ومساحتها 312.7 ألف كيلومتر مربع، كما يصل الناتج المحلي الإجمالي للفرد فيها إلى 31.4 ألف دولار

تحتل بولندا مراتب متقدمة في التقييمات العالمية ذات الصلة حيث حصلت على المركز الأول عالمياً في مؤشر الأمن السيبراني الوطني، والمركز 03 عالمياً في مؤشر الأمن السيبراني العالمي، فضلاً عن حصولها على المركز 43 في مؤشر التنمية الإلكترونية.

تم دراسة حالة بولندا من خلال تحليل المؤشر الوطني للأمن السيبراني وفق 21 محورًا، حيث حققت نتائج متميزة تمثلت في تحقيق 19% من مؤشرات السياسة الأمنية السيبرانية و49% من مؤشرات المساهمة الدولية و001% من مؤشرات حماية البنية التحتية الحيوي

فيما يتعلق بالمحور الأول «السياسات الأمنية السيبرانية»، فقد تحققت المؤشرات بنسبة 19%، ما يعكس وجود قيادة سياسية عليا معنية بالأمن السيبراني بالإضافة لوجود سياسات وخطط استراتيجية وطنية واضحة في هذا المجال.

أما في «محور المساهمة الدولية» فقد حققت المؤشرات بنسبة 49%، مما يبين التزام بولندا الدولي بمختلف اتفاقيات وتعهدات الأمن السيبراني إضافة لدعمها لبناء القدرات السيبرانية في دول أخرى وفي مجال «التعليم والتدريب» حققت المؤشرات نسبة 48%، ما يعكس ارتفاع مستوى الوعي والثقافة السيبرانية بين المواطنين البولنديين حيث ساهمت جهود بولندا الرامية لتعزيز كافة جوانب الأمن السيبراني في تفوقها عالميا، ما يمثل نموذجا يمكن للدول الأخرى الاستفادة منه

- **الدروس المستفادة من دراسة أفضل الممارسات:**

تعد دراسة الحالات الناجحة للدول الرائدة في مجال الأمن السيبراني من أهم الوسائل لاستقطاب أفضل الممارسات وتوظيفها في تعزيز قدرات الدول الأخرى وقد شكلت حالة بولندا مثالاً بارزاً يمكن الاستفادة منه، حيث حققت نتائج متميزة بفضل سياستها الشاملة في هذا المجال.

فعلى سبيل المثال، ساهم التركيز على بناء القدرات الوطنية من خلال التعليم والتدريب والبحث العلمي في رفع مستوى الوعي السيبراني لدى مختلف فئات المجتمع البولندي

كما سهل ذلك عملية الوقاية من المخاطر واستهداف الجهود نحو القطاعات ذات الأولوية مثل البنية التحتية الحيوية، كما لعب التنسيق الوطني الفعال بين كافة الجهات ذات العلاقة دوراً رئيسياً في تمكين بولندا من اعتماد سياسات وخطط استراتيجية شاملة أسهمت في تحقيق نتائج ملموسة.

علاوة على ذلك، فقد مكن التعاون الدولي الوثيق بين بولندا وشركائها من استيعاب أحدث الممارسات وتبادل الخبرات في مجالي استجابة الطوارئ السيبرانية ومكافحة الجرائم وبشكل عام، تعد حالة بولندا مثالاً ناجحاً يمكن للدول الأخرى أن تستفيد منه في تطوير قدراتها الوقائية والاستجابية تجاه التهديدات السيبرانية المستمرة.

- **التحديات المستقبلية:** مع تزايد التهديدات السيبرانية، تواجه برامج التوعية السيبرانية في القطاعات الحكومية تحديات متعددة، ومن أبرزها:

- **التطور المستمر للتهديدات السيبرانية:** وتيرة التطور في التهديدات السيبرانية متسارعة، مما يجعل الحاجة إلى تحديث مستمر لمحتوى التوعية والتدريبات الأمنية أمرًا ضروريًا.
- **التخصيص والشخصنة:** يعتبر تخصيص برامج التوعية لتتناسب مع احتياجات ومستويات مختلف المستخدمين تحديًا، إذ يتطلب فهمًا عميقًا للجمهور المستهدف وجميع المستويات الوظيفية والفكرية.
- **الأمن السيبراني للأجهزة المتصلة:** الزيادة في استخدام أجهزة إنترنت الأشياء (TOI) (تفتح المجال لمزيد من الهجمات، وهو ما يتطلب زيادة الوعي بأمن هذه الأجهزة وطرق التعامل معها
- **الجانب السلوكي والنفسي:** تغيير سلوكيات الأفراد وتحسين عاداتهم الأمنية يمثل تحديًا، حيث يتطلب فهمًا للعوامل النفسية والاجتماعية التي تؤثر على سلوك الأفراد.

الأمن السيبراني في الذكاء الاصطناعي: مع تزايد استخدام الذكاء الاصطناعي يوجه التركيز نحو أمن الأنظمة الذكية وكيفية توعية المستخدمين بالمخاطر المرتبطة بها

آفاق البحث المستقبلي: لمواجهة هذه التحديات، يمكن توجيه البحوث المستقبلية في مجال التوعية السيبرانية نحو عدة مسارات

- **تطوير محتوى ديناميكي وتكيفي:** البحث في تطوير محتوى تدريبي قابل للتكيف وفقًا للتغيرات في التهديدات السيبرانية والمستويات المختلفة للمستخدمين والمتعاملين

للخدمات الرقمية الحكومية

- **أساليب تعلم مبتكرة:** استكشاف استخدام أساليب تعلم جديدة مثل الواقع الافتراضي والألعاب التفاعلية لتعزيز الانخراط والحفاظ على المعلومات والاندماج في هذا البرامج غير التقليدية.
- **التصدي للتحديات النفسية:** الاستيعاب وفهم كيف يمكن للمعتقدات والعوامل النفسية أن تؤثر على سلوكيات الأمن السيبراني وكيف يمكن تصميم التحديات مستقبلية في مجال التوعية السيبرانية

مع تزايد التقدم التكنولوجي، تتطور التهديدات السيبرانية بصورة مستمرة، مما يتطلب جهودًا مضاعفة في مجال التوعية السيبرانية ومن التحديات الرئيسية التي يمكن التنبؤ بها:

- **تعقيد التهديدات:** التهديدات السيبرانية تصبح أكثر تعقيدًا، مما يجعل فهمها وتوعية الجمهور بشأنها أكثر صعوبة
- **التغيرات التكنولوجية السريعة:** التطورات السريعة في تكنولوجيات كالذكاء الاصطناعي وإنترنت الأشياء تخلق فجوات أمنية جديدة
- **التطور السلوكي:** مواكبة تطور سلوكيات المستخدمين وتفضيلاتهم، وخاصة مع تنوع الأجيال والثقافات.
- **الأمن بالتصميم:** صعوبة تطبيق مبادئ الأمن بالتصميم في كل المنتجات والخدمات الجديدة
- **الخصوصية والتنظيم:** التوازن بين التوعية وحماية خصوصية المستخدم مع التقيد بالقوانين والتنظيمات المحلية والدولية

الفصل الرابع

مناقشة النتائج والتوصيات

في السطور التالية، يعمد الباحث إلى مناقشة أهم النتائج التي تم التوصل إليها بخصوص التهديدات السيبرانية التي تتعرض لها الخدمات الرقمية للهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، والاستراتيجيات والتدابير الوقائية للتصدي لهذه التهديدات، وفعّالية برامج التوعية السيبرانية للموظفين والعاملين في الهيئة وبعد ذلك، يوضح الباحث أهم التوصيات التي يخلص إليها من دراسته لهذه القضايا جميعاً

وعليه، ينقسم هذا الفصل إلى مبحثين، هما: المبحث الأول بعنوان: مناقشة نتائج الدراسة، والمبحث الثاني بعنوان: توصيات الدراسة.

المبحث الأول

مناقشة نتائج الدراسة

تشير الإحصائيات إلى أن حوادث الاختراق والهجمات السيبرانية على الخدمات الرقمية الحكومية تتزايد بنسبة كبيرة سنويا وفقا لتقرير المخاطر العالمي 3202 من المنتدى الاقتصادي العالمي ، حيث أشار التقرير إلى أن الجريمة السيبرانية وعدم الأمان السيبراني تتصاعد بشكل ملحوظ بسبب الهجمات السيبرانية الأكثر عدوانية وتطورا و أصبحت تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة سببا في تميكن القراصنة في اختراق نظم تكنولوجيا المعلومات الحكومية بصورة أكثر فاعلية وسرعة في الانتشار والتأثير ويتفق ذلك مع ما ورد في تقرير المخاطر العالمي (2023)، كما يؤكده ما توصلت إليه دراسة مي الخليفة (3202) وطوابير عبدالجليل من أن الهجمات ستتزايد في التعقيد والخطورة، مما يستوجب تفعيل نظم دفاع سيبراني متطورة

- أهمية الأمن السيبراني للحكومات تكمن في قدرتها على ضمان استمرارية عمل الحكومة وحماية بياناتها وممتلكاتها وموظفيها من الهجمات السيبرانية بوجود التهديدات المتعددة مثل سرقة البيانات أو تلفها أو فقدانها، ويمكن أن تتعرض الحكومات لخسائر جسيمة وانتهاكات للخصوصية وعرقلة تقديم الخدمات الحكومية حيث تحمي ممارسة الأمن السيبراني الحكومات من تعطيل الأنظمة والشبكات الحكومية، والتي قد تؤدي إلى نقصان الثقة في الحكومة وتأثير سلبي على الاستقرار العام بالإضافة إلى ذلك، يحمي الأمن السيبراني من نشر المعلومات المضللة أو الدعاية التي يمكن أن تؤثر على

سلامة المجتمع واستقراره هو ما يتسق مع ما أكدته دراسة مي الخليفة (3202) التي أشارت إلى أن التحول الرقمي في الخدمات الحكومية يُسهم في تعزيز الأمن السيبراني بشرط وجود التزامات مؤسسية واضحة وموارد كافية لحماية المعلومات. كما يتفق ذلك مع دراسة خالد مهران التي شددت على أن غياب السياسات السيبرانية الصارمة يؤدي إلى تعرض الأنظمة الحكومية للشلل وتعطيل الخدمات الحيوية، مما يضعف ثقة الجمهور ويؤثر سلبًا على الاستقرار العام.

- تعد القرصنة من التهديدات المثيرة للقلق في الحكومات حيث تعرض متعامليها لهجمات: سرقة البيانات في الاعوام الماضية بشكل كبير ، وتعتبر سرقة البيانات الحساسة الناجمة عن الهجمات السيبرانية هي من بين التهديدات الأكثر أهمية من الناحية الاقتصادية على الدولة ، مع احتمال أن تؤدي إلى ضرر دائم للكيانات المعرضة للهجوم أو للمجتمع ككل في الامارات علاوة على ذل القرصنة الإلكترونية تمثل تهديدًا كبيرًا على الأمن القومي للدولة فقد تتيح القرصنة للمخترقين اختراق البنية التحتية الحيوية للدولة مثل المواقع الحكومية أو الوصول إلى البيانات السرية وتتفق هذه النتائج مع ما ورد في دراسة شيفتشينكو وآخرون، التي أكدت أن اختراق البيانات وكشف المعلومات غير المصرح بها من أكثر التهديدات شيوعًا، وتشكل خسائرها الاقتصادية خطرًا حقيقيًا على البنى التحتية والقطاعات الحساسة.
- تعتبر هجمات إنكار وحجب الخدمة من أخطر التهديدات الإلكترونية: التي تواجه المواقع والخدمات الحكومية حاليًا مما أدى إلى انقطاع الخدمة عن مئات الآلاف من المواطنين والمستخدمين وتتمثل خطورة هذا النوع من الهجمات في أنها لا تستهدف سرقة البيانات ولكنها تهدف في الدرجة الاولى إيقاف الخدمات أو جعلها غير قابلة للاستخدام من قبل المستخدمين كما أنها لا تتطلب مهارات عالية لتنفيذها مما يجعلها سهلة التوجيه والتنفيذ وقد يكون لهذه الهجمات أضرار اقتصادية واجتماعية كبيرة على الدولة خاصة إذا استمرت لفترات طويلة واستهدفت البنى التحتية الحيوية وتنسجم هذه النتيجة مع ما عرضته دراسة اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، التي صنّفت هجمات SoDD ضمن أخطر التهديدات على المؤسسات الحكومية، وأكدت أنها تؤدي إلى توقف الخدمات الحيوية، وتُستغل في كثير من الأحيان لزعزعة الثقة بالخدمات العامة .
- قطاع تكنولوجيا المعلومات في الاجهزة الحكومية بالدولة تواجه تحديات كبيرة في مجال إدارة مستخدم الهويات والوصول الى البيانات حيث يُعزى ضعف إجراءات التحكم

والرقابة إلى عدة عوامل، ومنها نقص الهياكل القائمة وعدم فعاليتها في إدارة الهويات للأنظمة والبرامج كما يظهر نقص في تطبيق إجراءات التحقق الثنائي، مما يجعلها أقل فعالية في منع الوصول غير المصرح به الى المعلومات و تعتبر تحديات إدارة الهويات والوصول أحد العقبات الرئيسية، خاصة في الحكومات التي تدير كميات كبيرة من المعلومات عبر الانظمة والخدمات المقدمة الى المتعاملين وقد شهدت الدولة تطورا هائلا في الخدمات السحابية و نموا مطردا خلال السنوات الأخيرة، بسبب خفض التكاليف والوصول إلى تقنيات وخدمات حديثة بسهولة ومرونة وتمكين الجهات الحكومية من العمل عن بُعد وتبادل البيانات فيما بينهم وتنعكس هذه النقطة في دراسة زمورة جمال وبن عيسى ليلى التي بيّنت أن الاعتماد المتزايد على الحكومة الإلكترونية يتطلب تعزيز النظم الأمنية على مستوى البنى التحتية والضوابط التقنية والتنظيمية ومن هنا، فإن ضعف إدارة الهوية الرقمية لا يُعد فقط مشكلة تقنية، بل يشكّل عائقًا استراتيجيًا في طريق حماية البيانات وضمان أمن الخدمات الرقمية الحكومية

- لا تزال معظم الهيئات والوزارات الاتحادية تفتقر لأعداد خطط واستراتيجيات شاملة لإدارة مخاطر الأمن السيبراني على المستوى الاستراتيجي حيث يواجه قطاع تكنولوجيا المعلومات في القطاع الحكومي تحديات كبيرة في مجال إدارة الأمن السيبراني على المستوى الاستراتيجي والتشغيلي ولا توجد استراتيجيات شاملة وفعالة لمواجهة التهديدات الرقمية المتزايدة نتيجة لعدة عوامل منها صعوبة تقييم المخاطر الناشئة بسبب حداثة مفهوم ومجال الأمن السيبراني كما أن نقص الكفاءات والخبرات البشرية المدربة في مجال الحماية الإلكترونية والسيبرانية يمثل عائقا آخر أمام العديد من الدوائر الحكومية بالإضافة إلى غياب التعاون والتنسيق بين الجهات الحكومية المعنية بسبب المنافسة المؤسسية مما يزيد من تعرض مؤسسات الدولة ومعلوماتها ومواطنيها لمخاطر الاختراق والهجمات السيبرانية.
- يواجه العديد من الوزارات والهيئات الحكومية صعوبات في الاستعانة بخبراء أمن معلومات وكفاءات مؤهلة لمواكبة التحديات الرقمية حيث يواجه قطاعات تقنية المعلومات تحديا كبيرا في الحصول على الكفاءات والخبرات المؤهلة في مجال أمن المعلومات والحماية الإلكترونية والسيبرانية وقد أشار خالد محمود مهران (2202) إلى أن عدم قدرة الهيئات الحكومية على منافسة القطاع الخاص في تقديم العروض المالية والحوافز يجعل جذب الكفاءات المؤهلة أمرًا بالغ الصعوبة وتعزى

هذه الصعوبات إلى عدة عوامل رئيسية، أهمها ندرة البرامج التدريبية والأكاديميات المختصة بهذا المجال وطبيعة عمل هذه الوظائف ذات المسؤولية العالية والضغوط النفسية الكبيرة تجعلها غير جاذبة بالنسبة للكثيرين ، وايضا قلة الوعي لدى بعض الجهات الحكومية بأهمية هذا الاختصاص لتعيين الكوادر الفنية المؤهلة مع تقديم برنامج سنوي يضمن استمرارية مستوى الكفاءة والجاهزية لهم وبالإضافة إلى عدم قدرة العديد من الهيئات الحكومية على منافسة القطاع الخاص في توفير العروض المادية والحوافز لهؤلاء الخبراء السيبرانيين واستقطابهم للعمل في المجال الحكومي.

- ضعف برامج تدريب موظفي القطاع الحكومي على المخاطر السيبرانية ساهم في زيادة حالات الإهمال البشري حيث يعد ضعف برامج التدريب على المخاطر وتهديدات الفضاء السيبراني من أهم العوامل التي ساهمت في ارتفاع حالات الإهمال البشري الذي يشكل تهديداً كبيراً للأمن الإلكتروني ونسبة كبيرة من الهجمات السيبرانية تستهدف العنصر البشري من خلال الرسائل الاحتيالية والبرمجيات الخبيثة ويرجع سبب ضعف برامج التدريب وعدم توفر الإمكانيات والخبرات اللازمة لدى العديد من الهيئات الحكومية لتصميم برامج تثقيفية فعالة بالإضافة لقلة الوعي لدى الكثير من المسؤولين بأهمية رفع مهارات الموظفين في هذا المجال السيبراني الحيوي نتيجة لضعف برامج التدريب كما أظهرت دراسات سابقة، مثل دراسة مي الخليفة (3202)، أن نسبة كبيرة من الهجمات السيبرانية تستهدف العنصر البشري، مما يبرز أهمية تعزيز الوعي والتدريب في هذا المجال وأصبح العديد من العاملين في القطاع الحكومي عرضة للوقوع فريسة لهجمات الاختراق الإنسانية مما يزيد من حالات الإهمال وعدم مراعاة الإجراءات الأمنية الأساسية والتعامل مع البريد الإلكتروني والروابط دون وعي كاف وقد تسبب ذلك في تسريب أعداد كبيرة من البيانات الحساسة والوثائق الرسمية كما سهل من عمليات الاختراق والوصول غير المصرح به للشبكات .
- تفتقر أنظمة الحوكمة الإلكترونية للعديد من الهيئات للتشريعات والسياسات الكافية واللازمة لحماية بيانات متعامليها وعلى الرغم من وجود ثورة رقمية متسارعة في قطاعات الحكومة المختلفة والسعي لتقديم خدماتها الإلكترونية عبر الإنترنت وتطبيقات الهواتف الذكية وزيادة اعتمادها على تقنيات المعلومات وقواعد البيانات الضخمة الا أنه ضعف ونقص الكفاءات القانونية المتخصصة في مجال حوكمة تكنولوجيا المعلومات والاتصالات في بعض الهيئات التشريعية يُعد من أبرز العوامل التي تسهم في تعريض بيانات المواطنين والمقيمين والقطاعات الحكومية لمخاطر أمنية كبيرة

والكثير من القوانين تفتقر إلى المرونة والشمولية، مما يترك ثغرات قانونية يستغلها المخترقون لتهديد خصوصية البيانات وسريتها كما أشار العديد من الباحثين، مثل دراسة اللجنة الاقتصادية والاجتماعية لغربي آسيا (2015)، إلى أن القوانين المتعلقة بالأمن السيبراني تفتقر إلى المرونة والشمولية، مما يترك ثغرات قانونية يستغلها المخترقون لتهديد خصوصية البيانات وسريتها ويتضح ذلك في عدم قدرة العديد من الهيئات على مواجهة التهديدات المتزايدة بسبب نقص الكفاءات القانونية المتخصصة.

- لم تواكب العديد من الهيئات الحكومية العديد من التطورات التكنولوجية الرقمية ونتيجة لعدم قدرة تلك الحكومات على مواكبة الابتكارات الرقمية أدى الى ظهور عدة ثغرات أمنية استغلها المهاجمون و تعاني الكثير في التكيف مع هذا العالم الرقمي الجديد ومواكبة التطورات الهائلة التي شهدها العالم خلال السنوات العشر الماضية ولم تستطع تلك الحكومات مواكبة انفجار مجالات الذكاء الاصطناعي ووغيرها من التقنيات المتطورة ونتيجة لعدم قدرة تلك الحكومات على مواكبة التغيرات التكنولوجية المتسارعة واستيعابها بشكل سليم، ظهرت العديد من الثغرات ونقاط الضعف في بنيتها التحتية لتكنولوجيا المعلومات مما ساعد المخترقين الإلكترونيين على استغلال تلك الثغرات واستهداف البيانات والنظم الحيوية بهجمات إلكترونية متكررة وقد أدى تعريض تلك الحكومات لمخاطر أمنية كبيرة وفق ما اشارت دراسة طواهير عبدالجليل (3202) إلى أن عدم التحديث المستمر للأنظمة والتقنيات المستخدمة في الهيئات الحكومية يجعلها عرضة لمخاطر أمنية كبيرة وإن الفشل في مواكبة الابتكارات الرقمية يعكس الحاجة الملحة لتطوير استراتيجيات شاملة تعزز من قدرات تلك الهيئات في مواجهة التهديدات المتزايدة.
- توجد فجوة كبيرة بين متطلبات الأمن السيبراني للخدمات الحكومية وميزانيات تمويلها بالنسبة للميزانية السنوية حيث تشهد ميزانيات الإنفاق على الأمن السيبراني في قطاعات الحكومة تحديات كبيرة، حيث توجد فجوة واسعة بين متطلبات حماية البنية التحتية والخدمات والموارد المالية المخصصة لهذا الغرض حيث أشار خالد محمود مهران (2202)، فإن ارتفاع تكاليف تنفيذ خطط الدفاع في الأمن الإلكتروني وتحديث البنية التحتية يجعل العديد من الهيئات غير قادرة على تأمين الميزانيات اللازمة بالرغم من التهديدات المتزايدة تعود هذه الفجوة في التمويل إلى عدة أسباب أهمها قلة الوعي لدى بعض المسؤولين بأهمية الاستثمار في مجال أمن المعلومات كما أن ارتفاع تكاليف تنفيذ خطط الدفاع في الأمن الإلكتروني وتحديث البنية التحتية تجعل العديد من الهيئات غير قادرة على توفير ميزانيات كافية بالإضافة مما يعرضها لمخاطر

هائلة في السمعة المؤسسية في حال تعرضها لهجمات سيبرانية.

- تُعتبر السياسة الحكومية الركن الأساسي للأمن السيبراني الحكومي، حيث تحدد الأهداف والاستراتيجيات الخاصة بالأمن السيبراني وتوجه عمليات تنفيذها وتشمل الشبكات والأنظمة والبيانات الحكومية بحيث يجب أن تكون البنية التحتية للحكومة محمية بشكل جيد ومؤمنة لمنع اختراقها وتعطيلها من قبل المهاجمين السيبرانيين وبالإضافة تعتبر القدرات البشرية للحكومة في مجال الأمن السيبراني عاملاً حاسمًا من خلال وجود موظفين حكوميين لديهم المعرفة والمهارات اللازمة للتعامل مع التهديدات السيبرانية وتنفيذ الإجراءات الأمنية اللازمة عند حدوثها .
- يعتبر إصدار توجيهات وسياسات تشجع المواطنين والمقيمين على اتخاذ إجراءات الأمن السيبراني يعد جزءًا هامًا من جهود الحكومات لتعزيز الأمن السيبراني كما أشار طواهير عبدالجليل (3202) إلى أن توعية المستخدمين بضرورة استخدام كلمات مرور معقدة تحتوي على مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز الخاصة تُعتبر من الخطوات الأساسية لتعزيز الأمان الشخصي حيث يمكن للحكومات تحسين وعي المواطنين وتشجيعهم على اتخاذ إجراءات الأمن السيبراني من خلال إصدار سياسات وتوجيهات واضحة وفعالة وتشمل هذه السياسات والتوجيهات تشجيع المواطنين والمقيمين على استخدام كلمات مرور قوية وآمنة لحساباتهم الإلكترونية وتجنب استخدام كلمات المرور الضعيفة التي يمكن تخمينها بسهولة ويجب أن تكون الكلمات المرور قوية وتحتوي على مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز الخاصة بالإضافة إلى ذلك، يجب على المواطنين والمقيمين تحديث البرامج والتطبيقات المستخدمة على أجهزتهم الإلكترونية بانتظام ، فإن تحديث البرامج يساعد في سد الثغرات الأمنية وتصحيح العيوب التي يمكن أن تستغلها الهجمات السيبرانية وعلاوة على ذلك، يجب على المواطنين والمقيمين تجنب مشاركة المعلومات الشخصية الحساسة عبر الإنترنت مع جهات غير موثوقة و يجب أن يكون للمستخدمين الوعي بأن المعلومات الشخصية مثل رقم الضمان وارقام الحسابات البنكية .
- من خلال التعاون الدولي، يمكن للحكومات في الدولة تبادل المعلومات الاستخباراتية والتحليلات الأمنية للكشف عن أنماط الهجمات السيبرانية والمصادر المحتملة لهذه الهجمات ويمكن للبلدان المشاركة في تبادل المعلومات المتعلقة بالثغرات الأمنية والتحديات السيبرانية المشتركة، وذلك لتعزيز فهمها والعمل المشترك في حلها بالإضافة إلى ذلك، يمكن للحكومات العمل مع المؤسسات الدولية مثل منظمة

الأمم المتحدة والاتحاد الأوروبي ومنظمات أخرى ذات صلة لتطوير إطارات قانونية وسياسات دولية لمكافحة الجرائم السيبرانية ويعمل التعاون المشترك على توحيد المعايير وتبادل الأفضليات وتطوير القدرات لمكافحة التهديدات السيبرانية العابرة للحدود وبالإضافة يمكن الاستعانة بالعمل مع فرق الاستجابة السريعة على المستوى الدولي لتحليل الهجمات السيبرانية وتقديم الدعم الفني للدول المتأثرة وتنظيم التمارين والمحاكاة للاستجابة للأزمات السيبرانية بالتعاون مع الشركاء الدوليين، وذلك لتعزيز القدرة على التصدي للهجمات والتعامل معها بشكل فعال وفق ما أظهرت دراسة اللجنة الاقتصادية والاجتماعية لغربي آسيا (5102) أهمية تعزيز التعاون بين الدول لمواجهة التحديات السيبرانية المشتركة، مما يساعد على تطوير استراتيجيات فعّالة لمكافحة الجرائم السيبرانية.

المبحث الثاني

توصيات الدراسة

تثير التهديدات السيبرانية للخدمات الحكومية الرقمية بالهيئة العديد من التساؤلات والإشكاليات التي تتطلب دراسة مستقبلية شاملة وأحد التساؤلات الرئيسية يتعلق بحجم تطور التهديدات السيبرانية في المستقبل والاستراتيجيات المتوقعة التي ستستخدمها المجموعات من القراصنة والمهاجمين على استهداف الخدمات الحكومية الرقمية ويستوجب أن نفهم كيف ستتطور التقنيات والأساليب التي يستخدمها المهاجمون للتغلب على إجراءات الأمان وحماية الحكومات من الهجمات بالإضافة إلى ذلك، هناك إشكاليات تتعلق بتقنيات الهجوم المتطورة التي يستخدمها المهاجمون فالعصر الرقمي شهد ولادة تقنيات الذكاء الاصطناعي وتعلم الآلة والتحليل الضخم للاختراقات ويمكن أن يمنح المهاجمين قدرات هائلة وهجومية قوية تجعل من الصعب اكتشافهم لذلك، ينبغي ان يتم دراسة كيف يمكن للهيئات الحكومية ان تحسن من قدراتها في مجال رصد واكتشاف واستجابة للهجمات السيبرانية المتطورة

تشكل البنية التحتية الرقمية للهيئات أيضًا نقطة ضعف محتملة يمكن استغلالها من قبل المهاجمين ويجب دراسة الثغرات والضعف المحتملة في البنية التحتية وتحديد الإجراءات اللازمة لتعزيز الأمان وتقوية البنية التحتية، مثل تحسين إجراءات المصادقة والتحقق وتعزيز أنظمة الحماية والرقابة عليها باستمرار

تؤثر الهجمات السيبرانية على خدمات الحكومة الرقمية بطرق متعددة، ولذا يجب دراسة التأثيرات المحتملة والتداعيات الاقتصادية والاجتماعية والسياسية لتعطل أو اختراق هذه الخدمات فقد ينتج عن ذلك انقطاع في تقديم الخدمات الحكومية الأساسية، وتأثير سلبي على الاستقرار السياسي والثقة في الخدمات الحكومية، وتكبد خسائر اقتصادية هائلة لذا، يجب دراسة كيفية تعزيز قدرة الحكومات على التعامل مع هذه التحديات وتقديم الخدمات بشكل مستمر وآمن.

هناك بعض الإشكاليات بالتشريعات والسياسات المتعلقة بالأمن السيبراني للخدمات الحكومية الرقمية يجب دراسة التشريعات والسياسات القائمة والمستقبلية التي يجب وضعها لتعزيز الأمن السيبراني وحماية البيانات والحقوق والحريات الأفراد يجب أن تكون هذه التشريعات والسياسات شاملة ومتوازنة للتصدي للتهديدات السيبرانية بشكل فعال

دون المساس بالحقوق والحريات الأساسية للمتعاملين في الدولة،

وفيما يلي التوصيات المهمة حول طرق التعامل مع التهديدات السيبرانية على الخدمات الحكومية الرقمية بالهيئة:

- **التشجيع على المبادرات الخاصة بالتحديات السيبرانية:** تعزيز الأمن السيبراني يتطلب مزيدًا من المشاركة والتحفيز من خلال إطلاق مسابقات الأمن السيبراني، حيث تعمل على تحفيز المحترفين لاكتشاف الثغرات وتحسين الأمان بشكل مستمر في أنظمة الهيئة وتطبيقاتها الرقمية ، مما يسهم في بناء شبكة مجتمعية قائمة على التعاون ويعتبر هذا النوع من المسابقات جزءًا من استراتيجية شاملة لبناء شبكة مجتمعية قائمة على التعاون وتعزيز الوعي الأمني في المجتمع وتعد مسابقات الأمن السيبراني فرصة للخبراء في مجال الأمن لاختبار مهاراتهم ومعرفتهم في التصدي للتهديدات السيبرانية حيث يتم توفير بيئة آمنة لهؤلاء الخبراء لاختبار قدراتهم في اكتشاف الثغرات وتحليلها وتطوير حلول لمعالجتها عن طريق تشجيع المشاركة في مثل هذه المسابقات، يتم دفع المحترفين للبقاء على اطلاع على أحدث التقنيات والتهديدات السيبرانية على الخدمات الرقمية الحكومية ، وبالتالي يتم تعزيز قدرتهم على التعامل مع تلك التهديدات.

يعد تشجيع التحديات السيبرانية حافز مهما أيضًا بالابتكار في مجال الأمن السيبراني حيث يعمل المشاركون في المسابقات على تطوير حلول جديدة وإبداعية لمعالجة تلك التهديدات السيبرانية ويتم تبادل المعرفة والخبرات بين المشاركين، مما يساهم في تطوير تقنيات وأدوات أمنية مبتكرة ويساهم هذا الابتكار في تعزيز قدرة خدمات الهيئة الرقمية على التصدي للتهديدات السيبرانية المتطورة وهي وسيلة فعالة لزيادة الوعي الأمني وتعزيز القدرات والامكانيات السيبرانية

- **استخدام الذكاء الاصطناعي للكشف عن التهديدات:** حيث عند استخدام الذكاء الاصطناعي في الكشف عن التهديدات السيبرانية فهي تعتبر أداة فعالة لتحسين أمان الأنظمة والشبكات الرقمية من خلال استخدام تقنيات الذكاء الاصطناعي، ويتم تحليل البيانات واكتشاف الأنماط غير الطبيعية التي تشير إلى وجود هجمات سيبرانية حالية ومستقبلية قد تحدث، مما يسمح بالتعرف المبكر على التهديدات وتفاديها قبل حدوث أضرار جسيمة وتستفيد تقنيات الذكاء الاصطناعي من قدرات التعلم الآلي وتحليل البيانات الضخمة لتحديد الأنماط المشبوهة والتصرف بفعالية من خلال تدريب نماذج الذكاء الاصطناعي على مجموعة واسعة من البيانات السليمة والمشبوهة، مما

يمكنها من التعرف على سلوكيات الهجمات والتنبؤ بنمط الهجمات المحتملة وايضا عندما يتم تحليل البيانات المتدفقة في الوقت الفعلي، يتمكن النظام من اكتشاف الأنماط غير الطبيعية وإصدار تحذيرات فورية للفرق الأمنية لاتخاذ التدابير اللازمة.

ويتيح استخدام الذكاء الاصطناعي للكشف عن التهديدات بسرعة ودقة أعلى في التحليل والاستجابة ويمكن للأنظمة الذكاء الاصطناعي معالجة كميات كبيرة من البيانات في وقت قصير وتحديد الأنماط المشبوهة بدقة عالية وبسرعة قياسية ويتمكن النظام من التعرف على الهجمات الجديدة وغير المعروفة وتحديد سلوكياتها المشتركة بناءً على نماذج التعلم الآلي السابقة، مما يسمح بتوجيه الجهود الأمنية بشكل فعال وتركز على المخاطر الحقيقية.

بالإضافة إلى ذلك، يمكن توظيف التكنولوجيا الذكاء الاصطناعي في تحسين عمليات الاستجابة والتعامل مع الهجمات السيبرانية من خلال اتاحة المجال لنظم الذكاء الاصطناعي في تقديم توجيهات وتوصيات للفرق الأمنية بشأن الإجراءات الوقائية والتدابير العاجلة المطلوبة للتصدي للهجمات وأيضًا استخدام الذكاء الاصطناعي في تحسين عمليات التحقيق وتحليل الحوادث السيبرانية، مما يساعد في تعزيز الاستجابة الفعالة وتقليل التأثيرات السلبية على الأنظمة الرقمية والتطبيقات الذكية للهيئة.

- **إشراك المجتمع في عمليات الأمن السيبراني :** من خلال إطلاق حملات توعية وبرامج تدريب للمجتمع، وتسعى إلى تعزيز الفهم حول امن الخدمات الرقمية والحسابات الشخصية عند التعامل مع انظمة وخدمات الهيئة الرقمية ، مما يمكّن المستخدمين من الحماية الذاتية وتعزيز ثقافة الإبلاغ عن الأنشطة الاشتباهية، ويعد إشراك المجتمع في عمليات الأمان السيبراني جزءًا مهما من الجهود الشاملة لتعزيز الأمن الرقمي من خلال إطلاق حملات توعية وبرامج تدريب للمجتمع، ويتم تعزيز الوعي والمعرفة حول أهمية الأمن السيبراني والتحديات التي يواجهها المستخدمون و بدوره يمكّن المستخدمين من اتخاذ إجراءات وقائية لحماية أنفسهم وتعزيز ثقافة الإبلاغ عن الأنشطة الاشتباهية وتشمل الحملات التوعوية توفير المعلومات والموارد التعليمية حول أهمية استخدام كلمات مرور قوية، والتحقق المتكرر من البرامج الضارة، وتحديث الأنظمة والبرامج بانتظام ويتم توضيح أيضًا طرق الاحتيال الشائعة مثل البريد الإلكتروني المزيف والتصيّد الاحتيالي والاحتيال عبر الهاتف، وكيفية التعرف عليها وتجنبها ويمكن أن تشمل الحملات التوعوية أيضًا نصائح للتعامل مع وسائل التواصل الاجتماعي بأمان والحفاظ على الخصوصية الشخصية.

وتقدم برامج التدريب فرصًا للمستخدمين لتعلم مهارات الأمن الرقمي والممارسات السيبرانية عن طريق تقديم تدريب عملي حول كيفية استخدام الأدوات والبرامج الأمنية، وكذلك التعرف على الهجمات الشائعة وكيفية التصدي لها ويمكن أن تشمل برامج التدريب أيضًا توجيهات حول إدارة وحماية البيانات الشخصية والتعامل مع الوثائق الرقمية بأمان ، وعندما يشارك المجتمع في هذه الحملات والبرامج، يتم تعزيز ثقافة الأمان والتعاون في مجتمع الامارات ويصبح المستخدمون أكثر وعيًا بالتهديدات السيبرانية ويكتسبون المهارات الضرورية لحماية أنفسهم وأجهزتهم وبالإضافة إلى ذلك، يتعزز الإبلاغ عن الأنشطة الاشتباهية، مما يمكن السلطات بالهيئة من اتخاذ التدابير اللازمة لمكافحة الجرائم السيبرانية.

ومن الجوانب المهمة أيضًا في توفير دعم فني ومساعدة للأفراد في حالة تعرضهم لهجمات سيبرانية وقد تتضمن إشراك المجتمع في عمليات الأمن السيبراني في توفير قنوات اتصال آمنة للإبلاغ عن الاختراقات الأمنية والأنشطة الاشتباهية بحيث تشجيع المجتمع على الإبلاغ عن أي تهديدات أمنية يشتبه في حدوثها، سواء كانت عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي أو أي منصة رقمية أخرى وبالتالي يكون هناك تواصل مستمر بين مقدمي الخدمات الرقمية بالهيئة والمجتمع، حيث يمكن للمستخدمين الحصول على التحديثات والإرشادات الأمنية الحالية.

- **تعزيز البحث والابتكار في الأمن السيبراني :**عبر تخصيص ميزانيات للبحث والابتكار، ندفع نحو تطوير افاق جديدة وفعّالة في مجال أمان السيبراني، مما يعزز التقدم المستمر ويعتبر تعزيز البحث والابتكار في مجال الأمن السيبراني هو جزء أساسي من الجهود الرامية إلى مكافحة التهديدات الرقمية المتزايدة وحماية الأنظمة والبيانات الحساسة بحيث يسمح تخصيص ميزانيات للبحث والتطوير في تقنيات متقدمة للكشف عن الهجمات السيبرانية والتصدي لها ويتم استخدام التحليل الذكي والذكاء الاصطناعي وتقنيات التعلم الآلي لتحليل أنماط السلوك الاعتيادية واكتشاف الأنشطة الغير مشروعة ومن خلال البحث والابتكار، يمكن تطوير أدوات وحلول تسهل الكشف عن الهجمات والتعامل معها بشكل سريع وفعال ويمكن تطوير أنظمة الاستجابة السريعة التي تتيح للمؤسسات التعامل مع الهجمات والتحقق من الانتهاكات واتخاذ إجراءات لمنع الأضرار القائمة والمستقبلية ويمكن استخدام ميزانيات البحث والابتكار لتطوير برامج تعزيز الوعي الأمني والتدريب للموظفين والمستخدمين وافراد المجتمع من خلال توفير التعليم والتدريب المناسب لهم لزيادة الوعي بالتهديدات السيبرانية

وتعزيز الممارسات الأمنية الجيدة في الهيئة ومجتمع الامارات وبالإضافة امكانية توظيف ميزانيات البحث والابتكار في تعزيز التعاون بين الشركات والمؤسسات الأمنية والأكاديمية والحكومية في الدولة من خلال تفعيل الشراكات والتعاون، يمكن تبادل المعرفة والخبرات والبيانات وتعزيز قدرات الاستجابة للتهديدات السيبرانية ويمكن لتخصيص ميزانيات للبحث والابتكار أن يؤدي إلى تطوير حلول متميزة تلبي احتياجات الأمن السيبراني المتنوعة بالهيئة لتغطي تطوير أنظمة متقدمة للكشف عن الهجمات، وأدوات لتعزيز التشفير والتوقيع الرقمي، وتقنيات لحماية البيانات الحساسة والتعامل مع التهديدات الجديدة مثل الهجمات الموجهة والاختراقات المتقدمة.

- **الاستثمار في التكنولوجيا الكمومية Technology Quantum:** هو واحد من الاتجاهات الرئيسية التي يتم يجب التركيز عليها لتعزيز الامن السيبراني في الهيئة من خلال استخدام مبادئ الفيزياء الكمومية في عمليات الحوسبة، يمكن تحقيق مستويات عالية من الأمان والفاعلية في تشفير وحماية البيانات تعتمد التكنولوجيا الكمومية على مفاهيم مثل التشويش الكمومي والمفاتيح الكمومية والاتصال الكمومي ويمكن استخدام التشويش الكمومي لحماية البيانات من الاختراقات، حيث يتم استخدام الخوارزميات الكمومية لتشفير المعلومات وتحميها من الهجمات السيبرانية القائمة والمستقبلية وايضا يمكن استخدام المفاتيح الكمومية لتأمين الاتصالات وتحقيق التشفير القوي باستخدام التكنولوجيا الكمومية، لتحقيق مزايا عديدة في مجال الأمن السيبراني فعلى سبيل المثال، يمكن للتشفير الكمومي أن يكون غير قابل للكسر بواسطة الحواسيب الكلاسيكية، مما يعزز أمان البيانات المرسلة والمخزنة للمستخدمين في انظمة الهيئة ويستخدم الاتصال الكمومي لتحقيق الاتصالات الآمنة والموثوقة بشكل لا يمكن تجاوزه من قبل الهجمات الخارجية مع ذلك، لا يزال العمل قائمًا على تطوير وتحسين التكنولوجيا الكمومية وتحتاج هذه التقنية إلى مزيد من البحث والتطوير لتحسين أداء الأجهزة الكمومية وتقنيات التشفير وتحقيق توافقها مع البنية التحتية الحالية للشبكات للهيئة ويتطلب الأمر تدريب الكوادر المتخصصة في هذا المجال وتعزيز التعاون بين القطاعات الأكاديمية والصناعية لدعم التطورات المستقبلية في التهديدات السيبرانية على الخدمات الرقمية .
- **إطلاق برامج «الهجمات التجريبية الوطنية»:** وهي مبادرة تهدف إلى تعزيز قدرة الهيئة مع الجهات المختصة على التصدي للهجمات السيبرانية من خلال تنظيم تدريبات وممارسات اختبارية منتظمة وتتضمن هذه البرامج إطلاق هجمات سيبرانية محاكية

لاختبار قدرة الهيئة على التعامل مع تلك الهجمات وتقييم استجابتها في ظروف واقعية وتحظى برامج «الهجمات التجريبية الوطنية» بأهمية كبيرة في سياق التهديدات السيبرانية المتزايدة فهذه الهجمات يمكن أن تكون متطورة ومستهدفة، وتشكل تهديدًا خطيرًا على الأمن القومي والاقتصاد والمؤسسات الحكومية ومن خلال تنظيم التدريبات الوطنية والهجمات التجريبية، يتسنى للحكومة تقييم قدراتها الحالية وتحديد النواقص والثغرات في أنظمتها وإجراءاتها الأمنية و تعمل برامج «الهجمات التجريبية الوطنية» على تعزيز الاستعداد والوعي السيبراني في الهيئة وتحسين الاستجابة للتهديدات السيبرانية ويمكنها الكشف عن الثغرات في الأنظمة والتطبيقات والبنية التحتية للهيئة ، ومن ثم تحسينها وتعزيز حمايتها كما تساعد على تطوير وتعزيز قدرات الفرق الأمنية وتدريبها على التعامل مع سيناريوهات الهجمات المتنوعة بالإضافة إلى ذلك، تسهم برامج «الهجمة التجريبية الوطنية» في تعزيز التنسيق والتعاون بين الجهات المعنية داخل الهيئة والجهات الخارجية في الدولة من توفر منصة لتبادل المعلومات والخبرات وتعزز التفاعل بين الجهات المختلفة.

- **نشاء وتشغيل مركز عمليات الامن السيبراني SOC:** وهو هيكل تنظيمي متخصص في رصد واستجابة وإدارة الأنشطة الأمنية في مراقبة الشبكات والأنظمة والتطبيقات والأجهزة للكشف عن أي أنشطة غير مشروعة أو مشتبه فيها والتعامل معها بشكل فعال ويعتمد مركز عمليات الأمن السيبراني على استخدام التقنيات المتقدمة وأدوات الأمان لتحليل السجلات والبيانات الأمنية، ورصد الحوادث الأمنية والتهديدات المحتملة، والتحقق من الحوادث واستجابتها، وإصدار تقارير دورية حول الأداء الأمني وتوصيات لتحسينه ، ويتم تجهيز المركز بأنظمة مراقبة متقدمة وأدوات تحليل التهديدات وتوظيف فريق متخصص من المحللين والمهندسين الأمنيين بالإضافة إلى ذلك، يجب توفير برامج تدريبية وتوعوية للموظفين لرفع الوعي وتعزيز المعرفة الأمنية وينبغي أيضًا تفعيل دور الشراكات مع خبراء الأمن السيبراني والجهات الخارجية المعنية بالأمن السيبراني، بما في ذلك NIST ومزودي الخدمات الأمنية الخارجية، من أجل تبادل المعلومات والخبرات وتحقيق أفضل مستويات الأمان السيبراني بالهيئة والتي ستساهم في تعزيز الثقة العامة في أنظمة الهيئة الرقمية وتعزيز استدامتها في ظل التهديدات السيبرانية المتزايدة .
- **تعزيز التشغيل الآلي للأمن السيبراني :** حيث يعد جزءًا أساسيًا من استراتيجيات الأمن الحديثة، ويتم استخدام التقنيات الحديثة مثل الأتمتة والذكاء الاصطناعي لتحسين قدرات الكشف والتحليل التلقائي، وبالتالي تقليل تأثير التهديدات على النظم والبيانات

باستخدام تقنيات الأتمتة، يمكن تنفيذ العديد من مهام الأمان بشكل آلي ومتكرر، مما يقلل من الاعتماد على التدخل البشري ويحسن الكفاءة والتنفيذ السريع على سبيل المثال، يمكن إعداد أنظمة الأمن للكشف التلقائي عن الأنشطة غير المشروعة أو الغير معتادة، واتخاذ إجراءات وقائية فورية مثل حظر الوصول أو تنبيه المشرفين وهذا يعزز القدرة على التصدي للتهديدات بشكل سريع وفعال بالإضافة ، يسهم في تحسين تشغيل الأمن السيبراني من خلال قدراته في التحليل الذاتي والتعلم الآلي ويمكن للأنظمة المدعومة بالذكاء الاصطناعي تحليل كميات ضخمة من البيانات وتحديد الأنماط والسلوكيات غير المعتادة التي يمكن أن تشير إلى هجمات سيبرانية ويمكن لهذه الأنظمة أيضًا تعلم النماذج الجديدة وتحديث القواعد والسياسات الأمنية بناءً على التحليلات والتقديرات المستمرة، ويعد الكشف السريع عن الهجمات والاستجابة الفورية من أبرز التأثيرات في تقليل التأثير السلبي للهجمات وتقليل فترة الاستجابة واستعادة النظم بالهيئة بشكل أسرع مع اهمية ان تكون هذه الأنظمة موثوقة وخالية من الأخطاء وتتمتع بمستوى عالٍ من الأمان نفسه.

- **إطلاق برامج «التحفيز بمكافأة الإبلاغ عن الثغرات الامنية « :** هو إحدى الاستراتيجيات الفعالة لتعزيز الأمن السيبراني و تتضمن هذه البرامج تقديم مكافآت أو مكافئات مالية للأفراد الذين يبلغون عن الثغرات الأمنية في النظم والبرمجيات التابعة للهيئة، أو الذين يساهمون بفعالية في تحسين الأمن السيبراني وتوفر برامج «مكافأة الإبلاغ» عددًا من الفوائد المهمة.

أولاً: تعزز ثقافة الإبلاغ وتشجع الأفراد على الإبلاغ عن الثغرات التي يكتشفونها بدلاً من استغلالها أو تجاهلها وتعمل هذه البرامج على تحويل الأفراد من محتملين للهجمات إلى شركاء في تعزيز الأمن السيبراني.

ثانيًا: تعزز برامج «مكافأة الإبلاغ» قدرة المنظمات على اكتشاف الثغرات وإصلاحها بسرعة من خلال تشجيع المبلغين على الإبلاغ عن الثغرات، حيث يمكن للهيئة أن تحصل على معلومات قيمة حول نقاط الضعف في أنظمتها وتطوير إصلاحات فعالة وهذا يقلل من فترة التعرض للهجمات ويحمي الأصول والبيانات المهمة

ثالثًا: تعمل برامج «مكافأة الإبلاغ» على تعزيز مفهوم مجتمع الأمن السيبراني حيث يشجع هذا النوع من البرامج على التعاون والتفاعل بين الباحثين الأمنيين والمؤسسات، ويساعد في بناء شبكة قوية من المهنيين المهتمين بالأمن السيبراني وبالتالي، يتم تبادل المعرفة والخبرات وتعزيز قدرات الأمن في الهيئة.

خاتمة:

سعت هذه الدراسة إلى فهم وتحليل التهديدات السيبرانية المحتملة التي قد تتعرض لها الخدمات الرقمية في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، وإجراء تقييم شامل لتأثير هذه التهديدات على سير عمل الخدمات الرقمية في الهيئة، وعلى جودة المقدمة للمواطنين والمقيمين في الدولة، ومن ثم استخلاص الدروس المستفادة وتطبيقها لتطوير منظومة عمل سيبرانية تحافظ على أمن الخدمات الحكومية الرقمية وتضمن استدامة عملها وتوفرها في المستقبل.

وقد تلخصت المشكلة البحثية لهذه الدراسة في السؤال التالي: كيف يمكن وضع الاستراتيجيات والتدابير الوقائية الناجحة للتعامل مع التهديدات السيبرانية الناشئة في الخدمات الرقمية للهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ، وكيف يمكن لبرامج التوعية السيبرانية للموظفين والعاملين في الهيئة الإسهام في تحسين مستوى الأمن السيبراني للخدمات الرقمية.

ولمعالجة هذه الإشكالية البحثية، استعان الباحث بالتحليل الوصفي للتهديدات السيبرانية الناشئة وتأثيراتها على الخدمات الرقمية، والملاحظة المباشرة للوضع السيبراني في الهيئة الاتحادية للهوية والجنسية والجمارك وأمن المنافذ كون الباحث يعمل بالهيئة منذ 2002، وأسلوب دراسة حالة الخدمات الرقمية بالهيئة، بالإضافة إلى إجراء مقابلات مع سعادة د. محمد الكويتي رئيس مجلس الامن السيبراني – مجلس الوزراء ، ومقابلة د.ابراهيم العلكيم خبير الامن السيبراني والذكاء الاصطناعي في حكومة ابوظبي وبالإضافة مقابلة المستشار عادل المهري والموظف عبدالعزيز النعيمي من هيئة تنظيم الاتصالات والخدمات الرقمية .

وقد تم تقسيم هذه الدراسة إلى أربعة فصول أساسية ، حيث تناول الفصل الأول الإطار النظري للدراسة من خلال عرض المقدمة ومشكلة الدراسة وتحديد أسئلتها البحثية و قدمت المقدمة خلفية موجزة عن موضوع التهديدات السيبرانية على الخدمات الحكومية الرقمية وأهداف الدراسة كما تم تحديد مشكلة الدراسة في انتشار الهجمات على الخدمات الحكومية الرقمية وشمل الفصل تحديد اربعة أسئلة بحثية رئيسية تتعلق بأنواع التهديدات واثرها والاستراتيجيات الفعالة في الحماية وطرق التوعية السيبرانية بالإضافة إلى تسليط الضوء على أهمية الدراسات السابقة في مجال التهديدات السيبرانية على الخدمات الرقمية ، وانتقلنا الى الفصل الثاني حول التهديدات السيبرانية الناشئة للخدمات الرقمية الحكومية بالهيئة حيث يتناول هذا الفصل أهم أنواع التهديدات السيبرانية الناشئة التي قد تشكل تهديداً للخدمات الحكومية الرقمية بالهيئة مثل هجمات إنكار وحجب الخدمة

والتجسس السيبراني وتهديدات سلاسل التوريد والخ ، ومن ثم تطرقنا حول آليات تحليل وتقييم مخاطر التهديدات السيبرانية الناشئة على الخدمات الحكومية الرقمية من خلال استخدام أدوات مثل تحليل القوة والضعف والفرص والتهديدات وتحليل المخاطر وإجراء تقييمات دورية للمخاطر وانتقلنا بعد ذلك الى مناقشة الفصل الثالث عن الاستراتيجيات الفعالة والتدابير المهمة لتعزيز الأمن السيبراني في الخدمات الحكومية الرقمية للهيئة حيث تناول المبحث الأول الاستراتيجيات والتدابير الوقائية للتعامل مع التهديدات مثل تطبيق سياسات الأمن والتشفير بينما ناقش المبحث الثاني أهمية توفير برامج توعية وتدريب مستمر للموظفين وأفراد المجتمع لرفع مستوى الوعي السيبراني وتحسين قدراتهم على التعامل مع المخاطر وعرجنا الى نهاية الدراسة في الفصل الرابع حول النتائج التي توصلت إليها الدراسة عن التهديدات السيبرانية على الخدمات الحكومية الرقمية بالهيئة حيث يلخص أهم أنواع التهديدات الناشئة وتأثيراتها المحتملة على الخدمات الرقمية كما يسرد النتائج المتعلقة بفاعلية الاستراتيجيات والتدابير الحالية للوقاية من هذه التهديدات ويختمها الفصل بمجموعة من التوصيات التي تسهم في تحسين مستوى الأمن السيبراني في الخدمات الحكومية الرقمية للهيئة على سبيل المثال، توصيات تتعلق بتدعيم البنية التحتية وزيادة التوعية الأمنية للموظفين وافراد المجتمع كافة

وقد توصلت الدراسة أنه من خلال تعزيز البحث والابتكار في مجال الأمن السيبراني يمكن من خلاله الدفع بقوة للجهود المبذولة في مكافحة التهديدات الرقمية المتزايدة وحماية الأنظمة والبيانات الحساسة وتدعيمها عن طريق تخصيص ميزانيات للبحث والتطوير للتوصل الى تطوير التقنيات المتقدمة للكشف عن الهجمات السيبرانية والتصدي لها في المستقبل والاستعانة في استخدام التحليل الذكي والذكاء الاصطناعي وتقنيات التعلم الآلي لتحليل أنماط السلوك الاعتيادية واكتشاف الأنشطة غير المشروعة لتسهل الكشف السريع والفعال عن الهجمات والتعامل معها مع الاهتمام بالاستجابة السريعة التي تسمح للمؤسسات بالتعامل مع الهجمات، والتحقق من الانتهاكات، واتخاذ إجراءات لمنع الأضرار الحالية والمستقبلية.

توصي هذه الدراسة بإنشاء وتشغيل مركز عمليات الأمن السيبراني(SOC) كجزء أساسي من استراتيجية الأمن السيبراني الشاملة حيث يعد SOC هيكلًا تنظيميًا متخصصًا ويهدف إلى رصد واستجابة وإدارة الأنشطة الأمنية في مراقبة الشبكات والأنظمة والتطبيقات والأجهزة والكشف عن أي أنشطة غير مشروعة أو مشتبه فيها والتعامل معها بشكل فعال ويعتمد المركز على استخدام التقنيات المتقدمة وأدوات الأمان لتحليل السجلات

والبيانات الأمنية، ورصد الحوادث الأمنية والتهديدات المحتملة، والتحقق من الحوادث واستجابتها بالإضافة إلى ذلك، يجب تجهيز المركز بأنظمة مراقبة متقدمة وأدوات تحليل التهديدات وتوظيف فريق متخصص من المحللين والمهندسين الأمنيين وينبغي أيضًا توفير برامج تدريبية وتوعوية للموظفين لرفع الوعي وتعزيز المعرفة الأمنية.

تثير هذه الدراسة العديد من التساؤلات والإشكاليات التي تظل في حاجة إلى إجابة مفصلة من بينها التالي:

- التهديدات السيبرانية الناشئة المحددة التي تشكل مخاطر على الخدمات الرقمية بالهيئة.
- أهم الاستراتيجيات والتدابير الوقائية الناجحة التي يمكن اتخاذها للتعامل مع التهديدات السيبرانية الناشئة في الخدمات الرقمية بالهيئة.

ربما تكون هذه التساؤلات أو الإشكاليات أو بعضها موضوعاً لدراسة أو دراسات أخرى يعكف عليها الباحث في المستقبل القريب من خلال إجراء دراسات إضافية للتعامل مع هذه التساؤلات والإشكاليات وتطوير استراتيجيات أمنية متطورة للحد من التهديدات السيبرانية بحيث تساهم هذه الدراسات في توفير الإجابات المطلوبة وتوجيه الهيئة في اتخاذ الإجراءات السليمة لحماية البنية التحتية الرقمية للهيئة وخدماتها

المراجع العربية

أولاً- المصادر الأولية

- برنامج الامارات للخدمة الحكومية المتميزة – حكومة دولة الامارات العربية المتحدة، 2 ديسمبر 2023.
- حكومة دولة الامارات العربية المتحدة، برنامج الإمارات للخدمة الحكومية المتميزة، 2 ديسمبر 3202،
- البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة، السلامة السيبرانية والأمن الرقمي، 10 ديسمبر 2023.
- الامان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياسية (اللجنة الاقتصادية والاجتماعية لغربي آسيا (الاسكوا) ، الامم المتحدة، نيويورك، 2015.

- المنظمة الدولية للمعايير ISO، « إدارة المخاطر - المبادئ والإرشادات»، 2018 .
- مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال أفريقيا. (د.ت.). الجريمة السيبرانية، مستخرج بتاريخ 18 يناير 2024.
- عبدالعزيز النعيمي، هيئة تنظيم الاتصالات والخدمات الرقمية، مقابلة (4 يناير 2024).
- د. محمد الكويتي، مجلس الامن السيبراني، مقابلة (24 يناير 2024).
- د. ابراهيم العلكيم، حكومة أبوظبي، مقابلة (22 يناير 2024).

ثانياً- الكتب والرسائل العلمية

- روس اندرسون، هندسة الأمان: دليل لبناء أنظمة موزعة موثوق بها(مدينة النشر: دار ويلي للنشر ، 0202) A3%gnireenignE+ytiruceS/ei-ne/moc.yeliw.www//:sptth idE+dr3+C2%smetsyS+detubirtsiD+elbadnepeD+gnidliuB+ot+ediuG+A+ 7872469111879-p-noit

ثالثاً- الدوريات

- مي الخليفة، «دور التحول الرقمي في تحقيق الامن السيبراني دراسة تطبيقية على وزارة العدل بدولة قطر»، مجلة البحوث الإدارية، المجلد 14، العدد 1، 3202، sptth:// 3401.475461.2202.osj/80612.01/gro.iod
- طواهير عبدالجليل، "استراتيجيات الأمن السيبراني كتحدي للتحول الرقمي بالمنظمات الحكومية مع الإشارة لتجربة دولة الإمارات العربية المتحدة " , مجلة الرسالة للدراسات الإعلامية، المجلد 7 ، العدد 1 , 2023 .
- 938812/elcitra/ne/zd.tsirec.pjsa.www//:sptth
- زمورة، جمال وابن عيسى، ليلى ، أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمة العمومية في الجزائر، مجلة البحوث الاقتصادية المتقدمة، المجلد 7، العدد 2، ص 414-924، 2202 . 4176141-MIB/liated/ten.aferame.hcraes//:sptth
- تشين زي، هان لي، شونغشو يو، «تصميم وتنفيذ بروكسي عكسي متحمل للثغرات بناءً على تقنية «esnefeD tegraT gnivoM» (DTM) لتطبيقات الحكومة الإلكترونية»، مؤتمر تكنولوجيا المعلومات والاتصالات الثاني لعام 1202 (CTCI)، نانجينغ، الصين، 1202، صفحات 072-372. 6269573/8102/5511.01/gro.iod//:sptth

- اشسان أنوري، دور الإدارة العامة في مكافحة جرائم الإنترنت: تحليل للأطر القانونية في إندونيسيا، المجلة الدولية للجريمة السيبرانية، المجلد 61، العدد 2، 2202. sptth://elcitra/lanruojemircrebyc/php.xedni/tpircsunem/moc.lanruojemircrebyc531/weiv
- خالد محمود مهران، الإجراءات التي تتخذها الدول في مواجهة مخاطر الاستخدام غير المشروع للفضاء الإلكتروني، المجلة القانونية، المجلد 41، العدد 6، 2202. 80612.01/629962.2202.WALJ
- شيفتشينكو، ب. ف.، جانغ، ج.، مالافاسي، م.، بيترز، ج. دبليو.، سوفرونوف، ج.، وتروك، س، طبيعة الخسائر من الأحداث ذات الصلة بالسيبرانية: فئات المخاطر وقطاعات الاعمال، مجلة الأمان السيبراني، المجلد 9، العدد 1، 3202. 3901.01/610cayt/cesbyc
- إريكا دي لونيرجان، جاكلين شنايدر، قوة المعتقدات في استراتيجية السيبرانية الأمريكية: التطور الدوري للردع والمعايير والتصعيد، مجلة الأمان السيبراني، المجلد 9، العدد 1، 3202 .21 IOD:3901.01/600dayt/cesbyc
- الزهراني، أ.، صافحي، أ.، الحبي، م.، المشاكل الأمنية الرئيسية لإنترنت الأشياء: التحديات واستراتيجيات الدفاع. المعاملة الدولية لمجلة الهندسة وإدارة التقنية والعلوم التطبيقية، المجلد 12 ، العدد 11، 2021 . sptth://moc.rgneut/V12A11S/fdp

رابعاً- المجلات والصحف

- مكي معمري، (3202، 9 نوفمبر)، مدارس أميركية تتعامل بجدية مع هجمات قراصنة الفدية، الامارات اليوم.
- رغدة البهي، «فيروس الفدية: الدفع أو الحذف والتشفير»، المركز المصري للفكر والدراسات الاستراتيجية، 01 نوفمبر 9102، sptth://yl.tib/3PtoX7DX
- هاني الأعصر، «الفضاء الإلكتروني.. تهديدات متزايدة تفوق القدرات التقليدية للدول»، مجلة درع الوطن، 3 أكتوبر 1202، sptth://yl.tib/3bXkZ5P
- محمد الكويتي، حوار ترينذ (2): النبض السيبراني، جلسة حوارية نظمها مركز ترينذ للبحوث والاستشارات، 72 يوليو 2022. sptth://www.ebutuoy.moc/v=32rpTdXRsn4?hctaw

-محمد الصوافي، «النبض السيبراني... كلنا مسؤول»، جريدة البيان، 92 يوليو 2202.

المراجع الإنجليزية

- latigiD .(7102) .A .T ,odraP & ,.R .J ,aícraG-liG (7102) .la te aícraG-liG .sdaorssorc eht gnidnif :hcraeser tnemeganam cilbup dna tnemnrevog 02.73091741/0801.01:iod .8711-5511 ,(8)91 ,weiveR tnemeganaM cilbuP 1817231.71
- trams ni ytiruces-rebyC .(8102) .E .H ,izahG & ,.N ,hcuobaaK ,.E .Z ,tebarM ,76 ,gnireenignE lacirtcelE ;pmA& sretupmoC .segnellahc dna yevrus :dirg .510.10.8102.gnecelepmoc.j/6101.01/gro.iod//:sptth .284-964
- yduts laciripme na :ti wenk ew erofeB» .sartimuD roduT dna ,alyeL ,egliB MCA 2102 eht fo sgnideecorP «.dlrow laer eht ni skcatta yad-orez fo .2102 .ytiruces snoitacinummoc dna retupmoC no ecnerefnoc
- A ?skcattarebyc elcihev ot dnopser srevird od woH» (2202) .la te rekraP scimonogrE dna srotcaF namuH eht fo sgnideecorP «yduts rotalumis gnivird .6051662231811701/7711.01:iod (2202) gniteeM launnA yteicoS
- lanoitanretni rof snossel :kcah sdniwralos ehT .(2202) .M ,illeraM ,ssorC deR eht fo weiveR lanoitanretnI .snoitazinagro nairatinamuh .4910002213836181s/7101.01/gro.iod//:sptth .4821-7621 ,(919)401
- a :eganoipse rebyc detroper ni erawlam fo elor ehT .(5102) .G ,negnaW //:sptth .112-381 ,(2)6 ,noitamrofnI .msinahcem dna tcapmi eht fo weiver 3810206ofni/0933.01/gro.iod
- kcaH tpeD etatS :secruoS .(01 hcraM ,5102) .S ,zcepukorP & ,.E ,zereP /scitilop/01/30/5102/moc.nnc.noitide//:sptth .scitiloP NNC .‹reve tsrow› eht lmth.xedni/reve-tsrow-kcah-tnemtraped-etats
- spag tnempoleved dna lacinhcet woh :2 sturts ehcapA .(8102) .J ,zczsuL .iod//:sptth .8-5 ,(1)8102 ,ytiruceS krowteN .hcaerb xafiuqe eht desuac .9-50003(81)8584-3531s/6101.01/gro
- ytiunitnoc ssenisub dnalgnE SHN « dnalgnE SHN .(3202) .N ,dnalgnE

//:sptth .dnalgnE SHN .kcatta yrCannaW :yduts esac tikloot tnemeganam kcatta-yrcannaw-yduts-esac/daer-gnol/ku.shn.dnalgne.www

- ssenerawa ytirucesrebyC .(1202) .H ,seraF & ,.M ,maraK ,.M ,redahK /0933.01/gro.iod//:sptth .714 ,(01)21 ,noitamrofnI .aimedaca rof krowemarf 71400121ofni
- tneve taerht rebyc gnitceteD .(0202) .C ,gnauH & ,.Z ,uiL ,.J ,oaG ,.Y ,gnaF //:sptth .2295 ,(71)01 ,secneicS deilppA .mtslib dna nncdi gnisu rettiwt morf 22957101ppa/0933.01/gro.iod
- noitamrofni elbaniatsus A .(2102) .M .L ,retneV & ,.M .M ,ffolE ,.K .C ,ewgnaW dna lacigolonhceT .ainaznat fo esac – tnemnrevog-e rof krowemarf ytiruces 83.01/gro.iod//:sptth .131-711 ,(1)81 ,ymonocE fo tnempoleveD cimonocE .691166.2102.31949202/64
- (tac) gniniart dna ssenerawa ytirucesrebyC .(2202) .G ,malA dna .M ,ijjiH //:sptth .3668 ,(22)22 ,srosneS .seeyolpme gnikrow etomer rof krowemarf 36682222s/0933.01/gro.iod
- .(2202) .A .M ,niassoH & ,.K ,leahciM ,.T .J .W ,eeL ,.R .M ,niddU ,.S ,retkA nevird-atad eht ni ytilibapac ssenerawa ytirucesrebyc gnizilautpecnoceR /7001.01/gro.iod//:sptth .hcraeseR snoitarepO fo slannA .ymonoce latigid 8-44840-220-97401s
- ytirucesrebyc fo srevird eht gnitagitsevnI .(2202) .M ,hatia'aM-lA cinortcelE ehT .nadroj fo esac eht :snoitazinagro cilbup ni tnemecnahne .iod//:sptth .(5)88 ,seirtnuoC gnipoleveD ni smetsyS noitamrofnI fo lanruoJ 32221.2dsi/2001.01/gro

-rebyc gnitarbilac :q-ved4rebyc .(1202) .K ,duaneR & ,.M ,kcooL ,.D .A ,agieV fo lanruoJ cinortcelE ehT .txetnoc yrtnuoc gnipoleved eht ni ssenerawa /2001.01/gro.iod//:sptth .(1)88 ,seirtnuoC gnipoleveD ni smetsyS noitamrofnI 89121.2dsi

-/ee.age.iscn//:sptth .xednI .(3202) .dnaloP :xednI ytiruceS rebyC lanoitaN

. /lp/yrtnuoc

-ytirucesrebyC .(2202) .V ,soluoikG & ,.K ,drågeeR ,.E ,datsyN ,.N ,yruhdwohC lanruoJ lanoitanretnI .seinapmoc erutcurtsarfni lacitirc naigewron ni gniniart /08281.01/gro.iod//:sptth .013-992 ,(3)21 ,gnireenignE ytiruceS dna ytefaS fo 403021.essji

- & ,.R .D ,nelluMcM ,.N ,reboG ,.A ,enyaP ,.S .M ,renurB ,.H .J ,oeS fo selpicnirp ecrofne ot ytilaer lautriv gnisU .(9102) .K .D ,ytrovarkahC -18 ,(1)01 ,noitacudE ecneicS lanoitatupmoC fo lanruoJ ehT .ytirucesrebyc .31/1/01/6314-3512.nssi/96322.01/gro.iod//:sptth .78

-//:sptth .muroF cimonocE dlroW .(11 yraunaJ ,3202) .3202 troper sksir labolG /3202-troper-sksir-labolg/snoitacilbup/gro.murofew.www

ملحق (1) : أسماء المصطلحات وتفسيراتها

م	المصطلح	التفسير
1	الهيئة	الهيئة الاتحادية للهوية والجنسية والاقامة والجمارك وامن المنافذ
2	الامن	حماية الأشخاص والممتلكات والمعلومات من التهديدات والمخاطر المحتملة
3	السيبراني	الفضاء للعالم الافتراضي والشبكات الإلكترونية
4	الامن السيبراني	الجهود والتدابير التي يتم اتخاذها لحماية الأنظمة الحاسوبية والشبكات الإلكترونية والبيانات من التهديدات السيبرانية
5	التهديدات	هي العوامل أو الأحداث التي يمكن أن تعرض الأنظمة الحاسوبية والشبكات الإلكترونية والبيانات للخطر
6	ENISA	منظمة وكالة الاتحاد الأوروبي للأمن السيبراني

ملحق (2) : أسماء المشرفين والخبراء الذين تم مقابلتهم

م	الاسم	اسم الجهة
1	المشرف عبد العزيز النعيمي	هيئة تنظيم الاتصالات والخدمات الرقمية
2	الخبير د. ابراهيم حمدان العلكيم	خبير الامن الالكتروني والذكاء الاصطناعي في حكومة ابوظبي
3	سعادة د. محمد الكويتي	رئيس مجلس الامن السيبراني – مجلس الوزراء

ملحق (3): أسئلة المقابلات مع هيئة تنظيم الاتصالات والخدمات الرقمية وحكومة أبوظبي:

السؤال الأول: ما هي التهديدات السيبرانية الرئيسية التي تواجهها الخدمات الحكومية الرقمية في الإمارات؟ بناءً على التقرير المعد من الهيئة ومقارنته مع التقارير الدولية في العالم والاجهزة الامنية المختصة تم الاجابة كالتالي : المشرف رقم (1) افاد انه نظرا للتطور التقني والتقدم التكنولوجي في الامارات وتنافسيتها مع دول العالم المتقدمة لاحظنا ابرز التهديدات المتكررة عبر السنوات مع تغير في الاساليب المتبعة في الاختراق وهي أولا : الوصول غير المصرح به ويعد تهديدًا خطيرًا للأنظمة الحكومية والخدمات الرقمية

وتمم من خلال خلال استغلال ثغرات في الشبكة أو استخدام أسماء مستخدمين وكلمات مرور مسروقة ،ثانيا : ومن هذه التهديدات التي ترتبط بمحاولة الاستيلاء على المعلومات الحساسة عن طريق المسح أو التجسس على الأنشطة الإلكترونية للأفراد أو المؤسسات الحكومية وهي المسح وعمليات التجسس ومحاولات الوصول الغير شرعية الى الانظمة الحكومية ، ثالثا : يعتبر التصيد والتزوير والتنكر من أكثر التهديدات انتشارا في الدولة حيث يتضمن التصيد الاحتيالي إغراء الأفراد بالمجتمع لتقديم معلومات شخصية من خلال رسائل البريد الإلكتروني المزيفة أو الروابط المشبوهة بالإضافه التزوير استخدام هويات للوصول إلى المعلومات أو الأنظمة الرقمية ويقوم بالتنكر كاستخدام هويات أو معلومات مزيفة للتمويه والتلاعب لحماية النفس من هذه التهديدات ، وأضاف ايضا الخبير (1) أن هجمات صيد الهوية عبر البريد الإلكتروني يمكن أن تستهدف اثنين من الأهداف الرئيسية من خلال الاستراتيجية الأولى فتتمثل في استهداف الأفراد الساذجين، أي الأشخاص الذين غالبًا ما يفتقرون إلى الوعي الكافي بأمور الأمان الإلكتروني حيث يقوم المهاجمون بإرسال رسائل بريد إلكتروني مزيفة تدعي عادة حاجة ماسة لتحديث معلومات الحساب أو تسجيل الدخول إلى حساباتهم و يستخدمون تقنيات اجتماعية متقنة لإغراء الأفراد وإقناعهم بالتفاعل مع هذه الرسائل المزيفة ويتضمن ذلك إدخال معلوماتهم الشخصية على صفحة احتيالية يتم توجيههم إليها عبر رابط بريد إلكتروني مزيف والاستراتيجية الثانية، فتستهدف الوظائف ذات المعلومات الحساسة يستهدف المهاجمون عادة الشركات والمؤسسات التي تحتوي على معلومات حساسة مثل المعلومات المصرفية أو معلومات العملاء ويتم إرسال رسائل بريد إلكتروني مزيفة إلى العاملين في هذه الوظائف، تدعي أنها من جهة موثوقة مثل الإدارة أو قسم تقنية المعلومات حتى يتم استخدام تقنيات تصيد الهوية المتطورة لإقناع الضحايا بالتفاعل مع الرسائل وتقديم معلوماتهم الشخصية أو تسجيل الدخول إلى الأنظمة الداخلية ، رابعا : تعتبر هجمات وثغرات تطبيقات الويب من التهديدات الشائعة وتستهدف هذه الهجمات عن طريق الثغرات في تطبيقات الويب الضعيفة أو الغير محدثة، مما يتيح للمهاجمين الوصول غير المصرح به إلى البيانات أو تنفيذ أو تعليمات ضارة بالأنظمة ، خامسا يعتبر استخدام الأنظمة أو التطبيقات غير المصرح بها تهديدًا مستمرا حيث يمكن أن يؤدي إلى تعريض الأنظمة الحكومية للثغرات ومخاطر الأمن .

السؤال الثاني : هل هناك زيادة في عدد وتعقيد التهديدات السيبرانية التي تستهدف البنية التحتية الرقمية للحكومة الإماراتية؟ ذكر المشرف (1) , انه على الرغم من تزايد اعتماد الحكومة الإماراتية على التكنولوجيا والخدمات الحكومية الإلكترونية الرقمية حيث

لوحظ زيادة عدد الأهداف الحيوية التي ستحاول الجهات والافراد المهاجمين الوصول إليها وكذلك لوحظ تتطور القدرات والإمكانات التقنية لدى المهاجمين واستمرار تطوير برامج الذكاء الاصطناعي عبر العالم يمنح المهاجمين القرصة لاستغلال الأدوات أكثر تقدما للوصول إلى البيانات والبنى التحتية الرقمية في الدولة وايضا استغلال المهاجمون لعلميات التجسس والتضليل عن طريق تطور في شبكات الجيل الخامس من الانترنت بسبب سرعة نقل البيانات بين الخدمات والخوادم الرقمية ، واكد الخبير (1) ان المهاجمين، يمكنهم من استخدام الذكاء الاصطناعي لتطوير برامج خبيثة متطورة وذكية قادرة على التلاعب بالأنظمة وسرقة المعلومات الحساسة ويمكن للذكاء الاصطناعي أن يتعلم من البيانات والسلوكيات لتوليد هجمات متكيفة تتلافى أنظمة الدفاع التقليدية .

السؤال الثالث: ما هي أبرز الجهات الهجومية التي تستهدف الخدمات الحكومية الرقمية في الإمارات؟ وما هي الأهداف المحتملة لهذه الهجمات ذكر المشرف (1) على أن التهديدات السيبرانية تمثل خطرًا جديًا يستهدف سرقة البيانات الحساسة وتعطيل الخدمات والبنى التحتية الحكومية الحيوية في الدولة ومن بين المهاجمين المتوقعين في هذا السياق تجد المجموعات الإرهابية ووكالات المخابرات في الدول المعادية والقراصنة المحترفين وتُسعى هذه المجموعات الإرهابية إلى استهداف الخدمات الحكومة الإماراتية من خلال تنفيذ هجمات إلكترونية انتقامية، نظرًا لسياستها الأمنية القوية ضد التطرف وحكمتها في علاقاتها مع دول العالم وتشمل أهداف المهاجمين في الحصول على تسريب المعلومات الحكومية أو خلق حالة من الفوضى من خلال هجمات حرمان الخدمة ولا يخفى على أحد عدائية الوكالات المخابرات في الدول المعادية في محاولة التجسس على البيانات الاستراتيجية والبنية التحتية للقطاعات الحيوية مثل النفط والطاقة في الدولة وفيما يستهدف القراصنة المحترفون اغراضهم المعروقة في سرقة البيانات الشخصية والمالية لأغراض إجرامية واضاف الخبير (1) انه يعتمد الهجوم على القطاع المستهدف حيث كلما كان الموقع مهم تكون المعلومات المستهدفة لها قيمة مادية عالية ومعنوية بالمجتمع بحيث دائما تجدب ترصد من المهاجمين للحصول على المعلومات عن طريق وسائل التهديدات السيبرانية الشائعة

السؤال الرابع: ما هي الثغرات الأمنية الأكثر استغلالاً في نظام الحكومة الرقمية في الإمارات؟ وما هي التدابير المتخذة لسد هذه الثغرات؟ اطلعنا المشرف (1) على أبرز الثغرات الأمنية التي يتم استغلالها في نظام الحكومة الرقمية بالإمارات ويمكن أن تختلف بناءً على البنية التحتية الرقمية والتقنيات المستخدمة ويشمل ذلك

- ضعف في إدارة الهوية والوصول: قد يحدث ضعف في إدارة الهوية والوصول مما يتيح للمهاجمين الوصول غير المصرح به إلى البيانات والموارد الحكومية الحساسة والمعلومات حول افراد المجتمع.
- **الثغرات في البرمجيات والتطبيقات:** يمكن أن تحتوي برمجيات وتطبيقات الحكومة الرقمية على ثغرات أمنية تسمح للمهاجمين بتنفيذ هجمات والتلاعب بالبيانات الشخصية والحكومية واضاف الخبير (1) أن لاحظ يتكرر هدا التهديد خاصه للأنظمة والتطبيقات المطور من مؤسسات الطرف الثالث ومن خارج الحكومات بحيث لا تمكن ضبط حكومة الامن السيبراني لديهم بسبب طبيعة عملها مع الجميع .
- **الهجمات المستهدفة على الشبكات:** يمكن للمهاجمين استغلال ثغرات في الشبكات الحكومية للوصول غير المصرح به إلى الأنظمة والبيانات الحساسة.
- **الهجمات الاجتماعية والهندسة الاجتماعية:** يستخدم المهاجمون تقنيات الهندسة الاجتماعية لخداع المستخدمين والحصول على معلومات حساسة أو تنفيذ هجمات فورية على الحسابات الشخصية والحكومية.

وذكر المشرف (1) أنه يجب أن تتخذ حكومة الدولة بعض من الإجراءات المتعددة لسد هذه الثغرات الأمنية الشائعة، وتشمل هذه التدابير

- **تنفيذ برامج الحماية والأمن الرقمي:** يتم تطبيق برامج الحماية والأمن المتقدمة للحد من الثغرات الأمنية وحماية البنية التحتية الرقمية.
- التدريب والتوعية: يجب ان يتم إطلاق برامج تدريب الموظفين تخصصية والمستخدمين عامة على أفضل الممارسات الأمنية والتوعية بمخاطر الهجمات السيبرانية وتقنيات الهندسة الاجتماعية.
- **إدارة الهوية والوصول:** يتم تطبيق إجراءات صارمة لإدارة الهوية والوصول للتحقق من هوية المستخدمين وتحديد صلاحيات الوصول بناءً على الاحتياجات والدور الوظيفي.
- **التحديثات الأمنية والصيانة الدورية:** يجب انه تتم تحديث البرمجيات والأنظمة بانتظام وتطبيق التصحيحات الأمنية لسد الثغرات المعروفة واكد عليها الخبير (1) انه يجب رصد جميع الثغرات في الانظمة ومعالجتها فورا لمنع تكرار الهجمات عليها وباستخدام (yrosivdA ecnegilletnI taerhT والتي تحدد الأنظمة المحددة أو البرامج أو التقنيات التي تعرض للخطر والمؤسسات في تحديد ما إذا كانوا معرضين للمخاطر ويحتاجون إلى اتخاذ إجراءات فورية.

السؤال الخامس : كيف يتم تصنيف وتقييم الأولويات في مجال الأمن السيبراني للخدمات الحكومية الرقمية في الإمارات؟ سرد لنا المشرف (1) ، التفاصيل المهمة حول كيفية يتم تحديد أولويات الأمن السيبراني للخدمات الحكومية الرقمية للدولة من خلال عملية منهجية لتقييم وتصنيف المخاطر والمتبعة في المؤسسات الحكومية وتبدأ هذه العملية بإجراء تقييم شامل للبنى التحتية والنظم الحكومية الرقمية الهامة، بهدف تحديد كافة الأصول والموارد التكنولوجية والبيانات الحيوية ومن ثم يتم تحليل مخاطر كل قطاع حسب درجة حيويته وتعرضه المحتمل للهجمات السيبرانية، واضاف الخبير (1) نوع القطاع يحدد طريقة ومجال الحماية المناسب له بحيث كلما كانت هناك قطاعات ووزارات عالية الاهمية كلما زادت عليها الاجراءات والتدابير الامنية السيبرانية واضافة المشرف (1) انه لتقدير تأثير مختلف السيناريوهات المحتملة عليه في حال وقوع أي هجمة وبناء على نتائج هذا التحليل، يتم تصنيف مخاطر كل قطاع وتحديد الأولويات، حيث تعتبر القطاعات ذات المخاطر العالية والتأثير الكبير أولوية قصوى ويتم تخصيص الموارد والاستثمارات اللازمة للحماية والاستجابة لهذه الأنظمة حسب ترتيب الأولويات، مع مراجعة دورية للتقييم بما يتلاءم مع التطورات المستمرة وبإشراف من الجهات الادارية والتقنية والفنية من الامن الكتروني والرقمي لكل قطاع وجهة حكومية في الدولة .

السؤال السادس: ما هي الآثار السلبية المتوقعة للاختراقات السيبرانية على الخدمات الحكومية الرقمية في الإمارات؟ ذكر المشرف (1) ، أن للاختراقات السيبرانية التي قد تطال أنظمة وبيانات الخدمات الحكومية الرقمية في الامارات آثار سلبية محتملة خطيرة فقد يؤدي تعطيل أو شلل الخدمات الحيوية مثل الرعاية الصحية أو البنية التحتية إلى فوضى معيشية كبيرة تؤثر على المجتمع بشكل سلبي واضاف ايضا الخبير (1) عند منع المستخدمين من الوصول إلى الخدمة الرقمية قد يسبب إحباطًا كبيرًا واستياءً من قبل الذين يعتمدون على الخدمة لأغراضهم اليومية و يشعر المستخدمون بالاستياء والغضب إذا لم يتم حماية معلوماتهم الشخصية بالشكل الصحيح ، ويمثل سرقة أو تسريب البيانات الشخصية والحيوية للمواطنين والمقيمين من انتهاكات للخصوصية وقد يستغلها المهاجمون في أنشطة إجرامية كذلك تعرض الدولة بالاختراقات بيئتها الرقمية لمخاطر جسيمة، وبالإضافة إلى إلحاق الخسائر الاقتصادية والسمعة بسبب تداعياتها وتكاليف إصلاح الأضرار واستعادة ثقة الجمهور حول خدماتها الرقمية

السؤال السابع: كيف يؤثر انقطاع الخدمات الحكومية الرقمية بسبب هجمات سيبرانية على المواطنين والشركات في الإمارات؟ ذكر المشرف (1) انه في حالة وجود انقطاع

الخدمات الحكومية الرقمية عن توافرها للمتعاملين بسبب وجود الهجمات السيبرانية قد يؤثر سلبًا على المواطنين والشركات في الدولة وعلى نطاق واسع ، فعند تعطل الخدمات الأساسية مثل التعليم أو الرعاية الصحية والخدمات المجتمعية والشخصية مثل تجديد الجواز واصدار التأشيرات والاقامات ، قد يهدد صحة وسلامة المواطنين والمقيمين وكما يعوق انقطاع الخدمات المالية والإدارية مثل الرسوم والتراخيص سير الأعمال وإنجاز المعاملات اليومية إلى جانب فقدان الثقة العامة بين المواطنين والشركات في كفاءة الحلول والخدمات الحكومية الرقمية المقدمة في الدولة وذكر ايضا الخبير (1) قد يؤثر انقطاع الخدمات الحكومية الرقمية بسبب هجمات سيبرانية على سمعة الإمارات وصورتها العامة في مجال التكنولوجيا والأمن السيبراني في حالة إذا لم يتم التعامل بفعالية مع هذه الهجمات وتحسين الأمن السيبراني، فقد يعتبر المجتمع الدولي أن الإمارات غير قادرة على حماية بياناتها ومصالحها الحكومية والاقتصادية

السؤال الثامن: ما هي التكاليف المحتملة للاستعادة وإصلاح الأضرار الناتجة عن الهجمات السيبرانية على البنية التحتية الحكومية الرقمية في الإمارات؟ قدر المشرف (1) التكاليف المحتملة عند تعرض الخدمات الرقمية للهجمات السيبرانية انها تكاليف مالية مرتفعة على الحكومة وبكل تأكيد قد تستهدف بنيتها التحتية الرقمية حيث تشمل هذه التكاليف إصلاح الأضرار المادية لأجهزة تكنولوجيا المعلومات والاتصالات ووقد يوجد تعويضات عن الخسائر الناتجة من فقدان أو تلف البيانات ، كما تستلزم عمليات استعادة الخدمات والبيانات وتطبيق تدابير الاستجابة الفنية تكاليف كبيرة حسب حجم الهجوم ، وعادة تتضمن النفقات المباشرة لفرق الطوارئ وكذلك الخسائر غير المباشرة أثناء فترات انقطاع العمل وبالإضافة إلى تكاليف تعزيز سبل الأمان طويلة الأمد لمواجهة التهديدات المتنامية وتزداد هذه التكاليف بشكل عام بحسب حجم الهجمة وطبيعة الأنظمة المستهدفة في الدولة واضاف الخبير (1) يعتبر في حالة وجود خطة إدارة الأزمات السيبرانية يمكن أن يقلل من تكاليف استعادة الأنظمة بعد وقوع هجوم سيبراني و توفر خطة إدارة الأزمات السيبرانية استجابة سريعة وتخطيطًا مسبقًا للتعامل مع الهجمات كما تشجع على التعاون والتنسيق بين الفرق المختلفة للحد من التأخيرات وتحليل الأزمة وتقييم الأضرار بفضل هذه العوامل، يمكن أن تساهم خطة إدارة الأزمات في تحقيق استجابة فعالة وتقليل التأثيرات السلبية وبالتالي تقليل تكاليف استعادة الأنظمة في الهيئات الحكومية .

السؤال التاسع: هل يمكن استعادة البيانات المسروقة أو التالفة نتيجة للاختراقات السيبرانية في الإمارات؟ وما هي التدابير المتبعة لذلك؟اكد المشرف (1) انه عادة يمكن استعادة

جزء من البيانات الحكومية التي تعرضت للسرقة أو التلف بسبب الاختراقات السيبرانية الواقعة عليها وذلك من خلال اتباع عدة تدابير وإجراءات وقائية مسبقا وأهمها وجود نسخ احتياطية متكررة للبيانات في أماكن ومواقع آمنة غير مرتبطة بالشبكات الحالية للمؤسسة الحكومية ، كما يمكن الاستعانة بتقنيات استعادة البيانات المتقدمة أو التعاقد مع شركات متخصصة في هذا المجال و تساعد محاولات التفاوض مع مرتكبي الاختراق في استعادة جزء من البيانات قبل نشرها او تسريبها على الشبكة العنكبوتية أما إذا طالت فترة الاختراق والهجوم السيبراني من دون اكتشافها فإن احتمال استرداد جميع البيانات يصبح أقل حظا ومع ذلك لا يضمن أي إجراء استعادة البيانات بنسبة 001 % وذكر الخبير (1) أن الوعي السيبراني من الإجراءات الرادعة والهامة لحماية البيانات في الهيئات الحكومية حيث يجب على المنظمات والأفراد أن يكونوا على دراية بمخاطر الهجمات السيبرانية وأهمية اتباع ممارسات الأمن المختلفة ويمكن تحقيق ذلك من خلال تنظيم حملات توعية وتدريبات منتظمة تهدف إلى زيادة الوعي وتعزيز المعرفة في مجال الأمن السيبراني و يتضمن ذلك توعية الموظفين والمستخدمين بالتهديدات السيبرانية المحتملة، وكيفية التعامل مع رسائل البريد الإلكتروني المشبوهة، والتعرف على الاحتيال الإلكتروني والهجمات الاحتيالية الأخرى من خلال زيادة الوعي السيبراني، يمكن الحد من احتمالية الوقوع في فخ الاختراقات السيبرانية والتقليل من تأثيرها المحتمل على البيانات المسروقة أو التالفة .

السؤال العاشر : ما هو تأثير الهجمات السيبرانية على سمعة الإمارات وموثوقيتها في مجال الخدمات الحكومية الرقمية؟استعرض المشرف (1) ابزر التأثيرات للهجمات السيبرانية على الدولة واهمها على الاطلاع الاضرار بسمعة الدولة ومستوى الثقة بقدراتها على تقديم الخدمات الحكومية الرقمية للمتعاملين بشكل آمن للضرر جراء الهجمات السيبرانية حيث قد ينخفض مستوى الطمأنينة لدى المواطنين والمؤسسات الخاصة تجاه حماية بياناتهم الشخصية، ما يؤثر سلبا على استخدام الخدمات الرقمية كما تظهر الدولة بمظهر غير مهني لعجزها عن ضمان الأمن السيبراني عن وقوع الهجوم وقد ينعكس ذلك على الاستثمار في قطاع تكنولوجيا المعلومات ، اضف ذلك وجود الانتقادات الداخلية والخارجية لسياساتها الأمنية السيبرانية كما اكد سابقا الخبير (1) ان سمعة الامارات من الاصول الغالية و الثمينة في الدولة وفي حالة وجود هجمات سيبرانية لم يكن لها هناك رادع وصد دفاعي قوي سيسبب في زعزعة الثقة بالخدمات الرقمية الحكومية .

السؤال الحادي عشر: ما هي أفضل الممارسات والإجراءات التي يجب اتباعها للوقاية من التهديدات السيبرانية على الخدمات الحكومية الرقمية في الإمارات؟ ذكر المشرف (1)

ان دولة الامارات تعتبر من الدول الرائدة في التنافسية الدولية ولديها سجل مشرف في التعامل مع الازمات حيث هناك عدة ممارسات وإجراءات أمنية مهمة لاتباعها كإحدى أفضل الطرق للوقاية من التهديدات السيبرانية على الخدمات الحكومية الرقمية ومن أهمها تنفيذ برامج وانظمة حكومية متكاملة لإدارة الدخول بالهويات الرقمية والوصول بحيث يتم تحديد صلاحيات معينة لكل مستخدم كما يجب تطبيق سياسات صارمة للتحكم بالبرامج والتطبيقات المسموح بها، وعلى الأخص تحديثات الأمن وانظمة التشغيل وبالإضافة إلى ضرورة اعتماد وتبني الانظمة الحديثة لتكنولوجيا الكشف والوقاية النشطة عن الحركات المشبوهة ومن دون الاعتماد على الحماية فقط وايضا يجب تدريب العاملين وافراد المجتمع وزيادة وعيهم بالتهديدات السيبرانية بشكل مستمر ومكثف وحديث وغير تقليدي ولا بد من عدم التغافل عن إجراء اختبارات للأنظمة بشكل مستمر من أجل الوقاية والاستجابة السريعة لأي حوادث الامن السيبراني واضاف الخبير (1) حولها انه يجب تنظيم تدريبات وممارسات اختبارية منتظمة وتتضمن هذه البرامج إطلاق هجمات سيبرانية محاكية لاختبار قدرة الهيئات الحكومية على التعامل مع تلك الهجمات وتقييم استجابتها في ظروف واقعية حتى يتسنى تقييم قدراتها الحالية وتحديد النواقص والثغرات في أنظمتها وإجراءاتها الأمنية لهدف تطوير تحسين الاستجابة للتهديدات السيبرانية واغلاق الثغرات في الأنظمة والتطبيقات والبنية التحتية للهيئات الحكومية .

السؤال الثاني عشر : كيف يمكن تعزيز قدرة الحكومة الإماراتية على الكشف المبكر عن التهديدات السيبرانية والتصدي لها؟ افاد المشرف (1) حول متطلبات عملية تعزيز قدرة الحكومة الاماراتية في مجال الكشف المبكر عن الهجمات السيبرانية والاستجابة لها بفاعلية من خلال تبني عدد من الإجراءات والمبادرات التقنية ومنها تطوير نظام مركزي متكامل لمراقبة البنية التحتية الحكومية الرقمية باستخدام تقنيات ذكية للكشف عن السلوكيات غير المسموح بها من الافراد والمؤسسات الحكومية ، وايضا شدد اهمية توفير التدريب والتأهيل للخبرات الوطنية في مجال استشراف التهديدات، فضلا عن الاستعانة بخبراء دوليين وتبادل الخبرات فيما بينهم وبالأخص التعاون مع الجهات ذات العلاقة وتبادل الاستخبارات والمعلومات السيبرانية ، واضاف أنه لا تقل أهمية تخصيص الموارد المالية والبشرية اللازمة لاستحداث أحدث تقنيات الرصد والتدقيق الدوري لنظم الأمن وفعالية خطط الاستجابة عند الاحداث السيبرانية واضاف الخبير (1) أن لتكنولوجيا الذكاء الاصطناعي فوائد كبيرة في مجال الأمان السيبراني، حيث تساهم في

التحليل التنبؤي للهجمات المحتملة، اكتشاف التهديدات المستهدفة، الاستجابة السريعة للتهديدات السيبرانية، والتحليل الفوري للأنشطة غير المعتادة وبفضل تلك الأدوات ، يتم تعزيز قدرة الأنظمة على الاستجابة والتصدي للهجمات السيبرانية وحماية البيانات والمعلومات الحساسة.

السؤال الثالث عشر: ما هو دور التدريب والتوعية في تعزيز الأمن السيبراني للخدمات الحكومية الرقمية؟

ذكر المشرف (1) انه يلعب دور التدريب والتوعية السيبرانية دورًا فاعلاً في تعزيز مستوى الأمن للخدمات الحكومية الرقمية بالإمارات حيث يتم من خلال برامج التدريب تزويد العاملين وافراد المجتمع بالمهارات والكفاءات اللازمة للتصدي للتهديدات السيبرانية كما يطلعهم على أحدث التقنيات وأفضل الممارسات الأمنية بالعالم ، مما يعزز قدراتهم في اكتشاف ومواجهة مخاطر الاختراق في كل الاوقات ، و بالنسبة للتوعية السيبرانية للمستخدمين،افاد فإنها تلعب دورًا وقائيًا هامًا من خلال نشر الوعي بأنواع التهديدات وكيفية التصرف بحكمة لتجنب الوقوع ضحية لهجمات الاحتيال أو البرامج الضارة وبالتالي يساهم في خلق ثقافة أمنية سليمة تدعم جهود حماية البنية التحتية للخدمات الحكومية الرقمية واضاف الخبير (1) انه التدريب يحسن من القدرات الفنية للموظفين العاملين في الخدمات الحكومية الرقمية هو جانب حيوي في تعزيز الأمن السيبراني ويعزز قدرة الموظفين على التفاعل مع التحديات الأمنية المعقدة ويمكنهم من تحليل وتقييم التهديدات بطرق فعالة وتطبيق إجراءات الحماية اللازمة ويساعدهم في تحديد الثغرات الأمنية المحتملة وتطبيق إجراءات الحماية والتشفير اللازمة للحفاظ على سلامة البيانات والمعلومات

السؤال الرابع عشر: ما هي الجهود التي تبذلها الإمارات لتطوير منظومة الأمن السيبراني للحكومة الرقمية؟ أكد المشرف (1) على علو مكانة الدولة في مجال الامن السيبراني حيث تبذل الدولة جهودا متواصلة لتطوير منظومة الأمن السيبراني لخدماتها الحكومية الرقمية باستمرار فقد أولت اهتماما بتخصيص ميزانيات لتمويل مشاريع بناء القدرات والكفاءات الوطنية في هذا المجال كمبادرة نبض ومبادرة قناص الاخيرة ، كما أنشأت العديد من الهيئات والمراكز المتخصصة بمراقبة الشبكات الحكومية واستشراف التهديدات السيبرانية لاكما تسعى لتعزيز التعاون مع القطاع الخاص والالتحاق بالاتفاقيات الدولية ذات الصلة وطرح الخبير (1) اهمية التعاقد مع شركات متخصصة في مجال الأمن السيبراني في القطاع الحكومي مما له من أهمية كبيرة في توفر هذه الشركات خبرة

وتخصص في مجال التهديدات السيبرانية وتقنيات الحماية، مما يساعد على مكافحة التهديدات السيبرانية المتزايدة بشكل فعال بفضل تحديثاتها المستمرة وتستطيع هذه الشركات مواكبة التطورات في مجال الأمن السيبراني وتطوير استراتيجيات الحماية المتقدمة بالإضافة إلى ذلك، يمكن للهيئات الحكومية تحقيق توفير في التكاليف من خلال الاستعانة بشركات متخصصة بدلاً من تكوين فرق داخلية للأمن السيبراني وتقدم هذه الشركات حلولًا مخصصة لاحتياجات الحكومة وتساعد في تعزيز الأمان السيبراني والتركيز على المهام الأساسية للحكومة

السؤال الخامس عشر: كيف يتم تحديث استراتيجيات الأمن السيبراني في الإمارات لمواجهة التهديدات المتطورة؟ طرح المشرف (1) افضل الطرق في تحديث الاستراتيجيات الوطنية للأمن السيبراني بالدولة من خلال استمرارية التغيير لمواكبة سرعة التغير في طبيعة التهديدات والتطورات التقنية ومن أجل ضمان فعالية هذه الاستراتيجيات في مواجهة التحديات الحالية والمستقبلية، يتم مراجعتها بشكل دوري مع اصحاب العلاقة من الجهات المختصة والمراكز المعتمدة و إجراء أبحاث استشرافية لاستكشاف أحدث أنماط الهجمات السيبرانية ، كما يتم التركيز على تطوير القدرات المحلية من خلال التدريب المستمر للكوادر ذات العلاقة وافراد المجتمع وتساعد عمليات المحاكاة السيبرانية والتقييم المستمر في اهمية قياس كفاءة الاستجابة للسيناريوهات الجديدة وهذا بلا شك يساهم في تحقيق مستوى عالٍ من الاستدامة الأمنية للبنية التحتية للخدمات الحكومية الرقمية في الامارات ، وذكر الخبير (1) انه لأعداد خطة الأمن السيبراني يتطلب من الجهات الحكومية مراعاة عدة عوامل مهمة منها تقييم المخاطر السيبرانية التي قد تواجه المؤسسة الحكومية وتحليل التهديدات المحتملة وثغراتها ويعتمد حجم المؤسسة على عوامل مثل حجم البيانات المخزنة ونوع الخدمات التي تقدمها التي تعمل فيها المؤسسة الحكومية كما يجب مراعاة الهيكل التنظيمي للمؤسسة وتناسب خطة الأمن السيبراني معه، بما في ذلك تعيين فريق متخصص في الأمن السيبراني فإذا كانت المؤسسة الحكومية كبيرة ويجب مراعاة الالتزامات التنظيمية المحددة التي تواجهها المؤسسة الحكومية للتوافق مع المعايير واللوائح المعمول بها .

السؤال السادس عشر: ما هي أهم الابتكارات التقنية المستخدمة في مجال الأمن السيبراني للحكومة الرقمية في الإمارات؟ عزز المشرف (1) من دور الدولة الريادي في استخدام أحدث التقنيات والابتكارات في مجال الأمن السيبراني لهدف رفع مستوى حماية بنيتها التحتية للخدمات الحكومية الرقمية فقد بدأت باستخدام تحليل البيانات الضخمة

وتقنيات الذكاء الاصطناعي لاستشراف التهديدات بكفاءة عالية من خلال المراكز الرقابية ، كما تلجأ لتقنيات حماية النقاط النهائية والحوسبة السحابية لتوفير خدمات الأمن كخدمة عالية الجودة ولحماية سرية البيانات فقد بادرت إلى تبني تقنيات التشفير المتقدمة في الدول المتقدمة وتسعى لتأهيل الكوادر البشرية القادرة على استثمار هذه التقنيات والابتكارات بكفاءة عالية لمواجهة تهديدات الفضاء السيبراني المتنوعة وبكل الاوقات وشدد الخبير (1) اهمية تبني الانظمة الذكية لرصد وتحليل السيبرانيات كأحد الجوانب الحاسمة في مجال الأمان السيبراني للحكومة الرقمية حيث تستخدم هذه الأنظمة المتخصصة في رصد وتحليل السيبرانيات لمراقبة الشبكات والأنظمة بشكل مستمر، وتقوم بتحليل سجلات الأحداث والمعلومات ذات الصلة، بهدف تحديد التهديدات المحتملة والسلوك غير العادي تعمل هذه الأنظمة على جمع وتحليل البيانات من مصادر متعددة، مثل سجلات الحركة والأحداث في الشبكة، وتقارير الاختراقات المحتملة، وتحليل الأنشطة غير المشروعة أو الغريبة لهدف تمكين مسؤولين الجهات الحكومية في اتخاذ إجراءات سريعة وفعالة للتصدي للتهديدات والتأكد من سلامة الأنظمة والبيانات الحكومية.

السؤال السابع عشر: كيف يتم توعية الموظفين والجمهور بأهمية الأمن السيبراني وكيفية التصدي للتهديدات السيبرانية في الإمارات؟ عدد المشرف (1) قائمة من المبادرات الحكومية في طرق توعية الموظفين والجمهور لأهمية الأمن السيبراني مثلا، تنظم وزارة الداخلية حملات توعوية مستمرة عبر وسائل الإعلام المختلفة للتحذير من أخطار الاحتيال عبر الإنترنت كما تصدر هيئة تنظيم الاتصالات والخدمات الرقمية دليلا إرشاديا شارحاً أفضل الممارسات الأمنية للمستخدمين والمؤسسات وبشكل مستمر وفي القطاع المصرفي مثلاً، تسعى بنوك الإمارات لنشر الوعي بين عملائها من خلال فعاليات توعوية ميدانية ، و تستخدم مجالس وقطاع الإعلام واجهات تواصل اجتماعي مبتكرة لنشر المحتوى التثقيفي بأسلوب ترفيهي ومحفز للتفاعل واضاف ايضا الخبير (1) لتوعية الموظفين والجمهور بأهمية الأمن السيبراني وتعزيز وعيهم بكيفية التصدي للتهديدات السيبرانية يمكن الاستعانة في استخدام اختبارات الوعي بالهجمات الاحتيالية المحاكاة المعروفة باسم «اختبار القرصنة الأخلاقية» أو «اختبار الصيد الاحتيالي» لقياس مستوى الأمان ومدى استعداد الموظفين للتعامل مع التهديدات السيبرانية وعادة تتضمن هذه الاختبارات إرسال رسائل بريد إلكتروني وهمية تحاكي هجمات الصيد الاحتيالي أو الفيشينغ (gnihsihP)، والتي تهدف إلى خداع المستلمين للنقر على روابط مشبوهة أو تقديم معلومات حساسة تستخدم هذه الرسائل الوهمية تقنيات التحايل والتلاعب الاجتماعي

لاختبار تصرفات واستجابة الموظفين وتعتبر هذه الاختبارات فعالة في تحديد نقاط الضعف والتحسينات اللازمة في سلوك الموظفين والتوعية بالتهديدات السيبرانية.

السؤال الثامن عشر: ما هي الشراكات المحلية والدولية التي تساهم في تطوير منظومة الأمن السيبراني للحكومة الإماراتية؟ ذكر المشرف (1) عدد من الشراكات المحلية والدولية والتي تعزز منظومة الأمن السيبراني للحكومة الإماراتية حيث على المستوى المحلي، وقعت هيئة تنظيم الاتصالات ولخدمات الرقمية عدد من اتفاقيات التعاون مع القطاع الخاص لتبادل الخبرات والمعلومات الاستخبارية حول التهديدات السيبرانية كما تعاونت مع الهيئات الأمنية في الدولة لبناء قدرات وطنية لتخصصات متقدمة وأطلقت العديد من البرامج التدريبية المشتركة بالتعاون مع الجامعات ومراكز البحـــــــوث واضاف الخبير (1) حول هذه النقطة انه من المهم تنظيم ورش عمل وتدريبات تطبيقية مشتركة بين الحكومة والشركات لتبادل المعرفة والممارسات الجيدة في مجال الأمن السيبراني للتناقش حول القضايا الحالية والتحديات ويتم توفير فرصة للمشاركين لتطبيق المفاهيم والتقنيات الأمنية في بيئة تدريبية حية ، وعلى الصعيد الدولي، فقد انضمت الإمارات إلى العديد من منظمات الأمن والتعاون في أوروبا واتفاقيات قمة العشرين بشأن الأمن السيبراني ، كما وقعت اتفاقات مع بلدان مثل بريطانيا والولايات المتحدة للتعاون في مجال مكافحة الجرائم وتبادل الخبرات كما توطدت العلاقات مع الشركات العالمية لدمج أحدث التقنيات والحلول في قطاع تكنولوجيا المعلومات وتوظيفها في الخدمات الرقمية بالدولة ويهدف خلال هذه الشراكات أن تستفيد الإمارات من الخبرات الدولية المتقدمة في تنفيذ أفضل الممارسات لحماية البنية التحتية لخدماتها الرقمية

ملحق (4): أسئلة المقابلات مع د. محمد الكويتي – رئيس مجلس الامن السيبراني – مجلس الوزراء

محور: الأمن السيبراني: تعريف وأهميته

1. **ما هي أهمية الامن السيبراني للحكومات، وماهي المخاطر التي تواجهها، وكيف يمكنها أن تحمي نفسها من هذه المخاطر؟**

أهمية الامن السيبراني للحكومات تمكن في ضمان استمرارية اعمالها وحماية بياناتها وممتلكاتها وموظفيها من الهجمات السيبرانية وتشمل المخاطر التي تواجهها الحكومات في مجال الامن السيبراني ما يلي:

- سرقة البيانات أو تلفها أو فقدانها، مما قد يؤدي إلى انتهاكات الخصوصية أو عرقلة

تقديم الخدمات الحكومية.

- تعطيل الأنظمة أو الشبكات الحكومية، مما قد يؤدي إلى انقطاع الخدمات أو فقدان الثقة في الحكومة.
- نشر المعلومات المضللة أو الدعاية، مما يؤثر على سلامة المجتمع أو استقراره.

ولكي تحمي نفسها من هذه المخاطر، يمكن للحكومات اتخاذ الإجراءات التالية:

- الاستثمار في تقنيات الامن السيبراني وبناء القدرات البشرية في هذا المجال.
- تطبيق الممارسات الأمنية الجيدة، مثل تأمين الشبكات والأنظمة وتدريب الموظفين على الأمن السيبراني.
- التعاون مع الحكومات الأخرى والمؤسسات الدولية لتبادل المعلومات وأفضل الممارسات.

محور: الركائز الأساسية للأمن السيبراني الحكومي

2. ما هي الركائز الأساسي للأمن السيبراني الحكومي، وما هي أهميتها، وكيف يمكن للحكومات تطبيقها بشكل فعال؟ وما هي أهم التحديات التي تواجه الحكومات في تطبيقها؟

- السياسة هي الركن الأساسي للأمن السيبراني الحكومي، والتي تحدد أهداف الأمن السيبراني وأطر عمل تنفيذها.
- البنية التحتية، والتي تشمل الشبكات والأنظمة والبيانات الحكومية.
- القدرات البشرية، والتي تشمل مهارات ومعرفة الموظفين الحكوميين في مجال الأمن السيبراني.

تمكن أهمية هذه الركائز في ضمان تحقيق الأمن السيبراني على مستوى الحكومات ككل الا أنها تواجه مجموعه من التحديات ومن ضمنها:

- عدم وجود تنسيق كافٍ بين مختلف الجهات الحكومية المسؤولة عن الأمن السيبراني.
- عدم كفاية الموارد المالية والبشرية المخصصة للأمن السيبراني.
- عدم وجود وعي كافٍ للأمن السيبراني بين الموظفين الحكوميين.

محور: التحديات السيبرانية الأكثر شيوعاً Trends

3. ما هي التهديدات السيبرانية الأكثر شيوعاً التي تواجه الحكومات؟

تواجه الحكومات مجموعة متنوعة من التهديدات السيبرانية، ومن أبرزها:

- **هجمات الفدية:** وهي الهجمات التي يقوم فيها ممثلو التهديد باختراق نظام معلومات الحكومة ومطالبتها بدفع فدية مقابل فك تشفير البيانات أو استعادة الوصول إليها. ووفقاً لتقرير صادر عن شركة «آي إس آر جي سي (ISRGC)» فإن نسبة الهجمات الناجحة بهذه الطريقة بلغت 62% في عام 2023.
- **هجمات حجب الخدمة SoDD**: وهي الهجمات التي تهدف إلى تعطيل أو شلل أنظمة المعلومات الحكومية، مما يمنع المستخدمين من الوصول إليها. ووفقاً لتقرير صادر عن شركة « آي إس آر جي سي (ISRGC)»، فإن نسبة الهجمات الناجحة بهذه الطريقة بلغت 22% في عام 2023.
- **هجمات التصيد الاحتيالي:** وهي الهجمات التي يتم فيها إرسال رسائل إلكترونية أو رسائل نصية مزيفة تبدو وكأنها من مصادر موثوقة، بهدف خداع المستخدمين لإدخال بيانات حساسة مثل كلمة المرور أو معلومات بطاقة الائتمان. ووفقاً لتقرير صادر عن شركة «آي إس آر جي سي (ISRGC)»، فإن نسبة الهجمات الناجحة بهذه الطريقة بلغت 81% في عام 2023.
- **هجمات البرمجيات الخبيثة:** وهي البرامج الضارة التي يتم تصميمها لإلحاق الضرر بأنظمة المعلومات، مثل سرقة البيانات أو تخريبها ووفقاً لتقرير صادر عن شركة «آي إس آر جي سي (ISRGC)»، فإن نسبة الهجمات الناجحة بهذه الطريقة بلغت 51% في عام 2023.

4. كيف يمكن للحكومات حماية نفسها من هذه التهديدات؟ وما هو دور الحكومات في توعية المواطنين بمخاطر الهجمات السيبرانية؟

تتمثل أفضل طريقة لحماية الحكومات من التهديدات السيبرانية في اتباع نهج شامل يتضمن ما يلي

- بناء بنية تحتية أمنية قوية: من خلال الاستثمار في تقنيات وممارسات الأمن السيبراني الحديثة، مثل أنظمة الحماية من البرامج الضارة وأنظمة اكتشاف التسلل.
- رفع مستوى الوعي الأمني لدى الموظفين: من خلال تدريب الموظفين على كيفية

التعرف على التهديدات السيبرانية وكيفية حماية أنفسهم من الوقوع ضحيتها.

- التعاون مع الجهات الحكومية الأخرى وشركات القطاع الخاص: من أجل تبادل المعلومات والمعرفة حول التهديدات السيبرانية والتعاون في جهود الاستجابة لها حيث تلعب الحكومات دوراً مهماً في توعية المواطنين بمخاطر الهجمات السيبرانية، وذلك من خلال:
- **نشر حملات توعوية:** تستهدف هذه الحملات جميع فئات المجتمع، وتتضمن معلومات حول أنواع التهديدات السيبرانية وكيفية حماية أنفسهم منها.
- **أنشاء برامج تعليمية:** تقدم هذه البرامج معلومات حول الأمن السيبراني للطلاب والموظفين وغيرهم من المواطنين.
- **التعاون مع وسائل الاعلام:** لنشر الوعي حول التهديدات السيبرانية وكيفية مواجهتها.

محور: التحول الرقمي في الامارات

5. **كيف يؤثر التحول الرقمي على أمن الحكومات؟ ما هي المخاطر والتحديات التي تواجهها الحكومات في ظل التحول الرقمي؟**

يؤثر التحول الرقمي على أمن الحكومات بشكل كبير، حيث يعرضها إلى مجموعة من المخاطر والتحديات الجديدة، ومن أهمها:

- **زيادة الاعتماد على الأنظمة والشبكات الإلكترونية:** يؤدي التحول الرقمي إلى زيادة الاعتماد على الأنظمة والشبكات الإلكترونية في تقديم الخدمات الحكومية، مما يمثل هدفهاً جذاباً للهجمات السيبرانية.
- **ارتفاع مستوي تعقيد البنية التحتية الرقمية:** تصبح البنية التحتية الرقمية للحكومات أكثر تعقيداً مع التحول الرقمي، مما يجعلها أكثر عرضة للاختراق.
- **انتشار تقنيات جديدة:** تنتشر تقنيات جديدة في مجال الأمن السيبراني، مما يتطلب من الحكومات مواكبة هذه التطورات وامتلاك القدرات اللازمة للتعامل معها.

محور: آليات الحماية

6. ما هي الإجراءات التي يمكن للحكومات اتخاذها لضمان أمنها السيبراني؟

هناك مجموعة من الإجراءات التي يمكن للحكومات اتخاذها لضمان أمنها السيبراني، ومن أهمها:

- **وضع استراتيجية للأمن السيبراني:** يجب على الحكومات وضع استراتيجية شاملة للأمن السيبراني، تحدد أهدافها وإجراءاتها.
- **الاستثمار في الأمن السيبراني:** يجب على الحكومات الاستثمار في الأمن السيبراني، من خلال توفير بنية تحتية رقمية آمنة وموظفين مؤهلين.
- **التعاون الدولي:** يجب على الحكومات التعاون معاً على المستوى الدولي لتبادل المعلومات والتجارب ومواجهة التهديدات السيبرانية.

7. كيف يمكن للحكومات أن تستثمر في بناء القدرات البشرية في مجال الأمن السيبراني لتعزيز هذه الآليات؟

يمكن للحكومات أن تستثمر في نباء القدرات البشرية في مجال الأمن السيبراني من خلال ما يلي

- **التعليم والتدريب:** يجب أن تستثمر الحكومات في التعليم والتدريب في مجال الأمن السيبراني. ويشمل ذلك توفير فرص التعليم والتدريب للموظفين الحكوميين، والتعاون مع المؤسسات التعليمية لتوفير برامج تعليمية في هذا المجال.
- **التوظيف والتطوير المهني:** يجب أن تدعم الحكومات توظيف وتطوير المتخصصين في مجال الأمن السيبراني. ويشمل ذلك تقديم حوافز للموظفين الحكوميين للعمل في مجال الأمن السيبراني، وتوفير فرص التطوير المعني للموظفين في هذا المجال.
- **البحث والتطوير:** يجب أن تستثمر الحكومات في البحث والتطوير في مجال الأمن السيبراني. ويشمل ذلك دعم الأبحاث التي تركز على تطوير تقنيات أمان جديدة، والتعاون مع الجامعات والشركات في مجال البحث والتطوير في مجال الآمن السيبراني.

محور: التحول السحابي والخدمات الرقمية

8. كيف يمكن للحكومات أن تستفيد من الاستثمارات في تقنيات الأمن السيبراني والتحول السحابي في ظل المخاطر التي تصاحب التحول السحابي؟

هناك العديد من الفرص لاستفادة الحكومات من الاستثمار في تقنيات الأمن السيبراني والتحول السحابي، من خلال

- **تحسين الكفاءة التشغيلية:** يمكن للحكومات استخدام تقنيات الأمن السيبراني لتحسين كفاءتها التشغيلية من خلال أتمتة المهام وتحسين مشاركة البيانات واتخاذ القرارات.

- **تعزيز الابتكار:** يمكن للحكومات استخدام تقنيات الأمن السيبراني والتحول السحابي لتعزيز الابتكار من خلال إنشاء بيئات أكثر أماناً وتعاوناً للموظفين والمؤسسات.
- **تحسين الخدمات الحكومية:** يمكن للحكومات استخدام تقنيات الأمن السيبراني والتحول السحابي لتحسين الخدمات الحكومية من خلال توفير خدمات أكثر سهولة وكفاءة وأماناً للمواطنين.

محور: أمثلة على أسئلة محددة

9. ما هي خطط دولة الامارات العربية المتحدة لتعزيز أمنها السيبراني في السنوات القادمة؟

تخطط دولة الامارات العربية المتحدة لتعزيز أمنها السيبراني في السنوات القادمة من خلال عدد من المبادرات، بما في ذلك:

- **تفعيل مركز العمليات الوطني الأمني NSOC:** العمل على شمول كافة القطاعات الحيوية في الدولة بمركز عمليات أمن سيبراني مركزي، لمواجهة التهديدات السيبرانية والتصدي لها.
- **تعميم السياسات المتعلقة بالأمن السيبراني:** على كافة الجهات العاملة في الدولة والعمل على امتثالهم لهذه السياسات.
- **تعزيز التعاون الدولي في مجال الأمن السيبراني:** تسعى دولة الامارات العربية المتحدة إلى تعزيز التعاون الدولي في مجال الأمن السيبراني، من خلال المشاركة في المنتديات الإقليمية والدولية، وتوقيع اتفاقيات التعاون مع الدول الأخرى.
- **رفع مستوى الوعي بالمخاطر السيبرانية:** تسعى دولة الامارات العربية المتحدة إلى رفع مستوى الوعي بالمخاطر السيبرانية لدى الافراد والجهات المعنية، من خلال إطلاق حملات توعية مثل النبض السيبراني وتقديم التدريبات ذات الصلة.

10. ما هي التحديات التي تواجه دولة الامارات العربية المتحدة في مجال الأمن السيبراني؟

تواجه دولة الامارات العربية المتحدة عدداً من التحديات في مجال الأمن السيبراني، يمكن إجمالها في النقاط التالية

- **تزايد التهديدات السيبرانية:** تتعرض دولة الامارات العربية المتحدة، كما هو الحال بالنسبة لدول العالم الأخرى، إلى مجموعة متنوعة من التهديدات السيبرانية بما في ذلك الهجمات السيبرانية التي تستهدف البنية التحتية للقطاعات الحيوية، والهجمات

التي تستهدف سرقة البيانات أو نشر معلومات مضللة.

- **تطوير تقنيات الأمن السيبراني:** يشهد مجال الأمن السيبراني تطوراً سريعاً، حيث تطرح الشركات المتخصصة في مجال الأمن السيبراني باستمرار تقنيات جديدة للتصدي للتهديدات السيبرانية: يتطلب هذا من دولة الامارات العربية المتحدة مواكبة التطورات في مجال الأمن السيبراني، توفير الإمكانيات اللازمة للاستفادة من هذه التقنيات.

11. والمؤسسات الدولية لتعزيز أمنها السيبراني؟

يمكن لدولة الامارات العربية المتحدة أن تتعاون مع الحكومات الأخرى والمؤسسات الدولية لتعزيز أمنها السيبراني من خلال عدد من الآليات، ويمكن إجمالها في النقاط التالية

- **التعاون في مجال البحث والتطوير:** يمكن لدولة الامارات العربية المتحدة التعاون مع الحكومات الأخرى والمؤسسات الدولية في مجال البحث والتطوير في مجال الأمن السيبراني، بهدف تطوير تقنيات جديدة للتصدي للتهديدات السيبرانية.
- **تبادل المعلومات والمعرفة:** يمكن لدولة الامارات العربية المتحدة التعاون مع الحكومات الأخرى والمؤسسات الدولية في مجال التدريب والتطوير للكوادر المتخصصة في مجال الأمن السيبراني.

محور: التهديدات السيبرانية على الخدمات الحكومية الرقمية في الامارات:

12. هل هناك زيادة في عدد وتعقيد التهديدات السيبرانية التي تستهدف البنية التحتية الرقمية للحكومة الإماراتية؟

نعم، هناك زيادة في عدد وتعقيد التهديدات السيبرانية التي تستهدف البنية التحتية الرقمية للحكومة ويرجع ذلك إلى عدة عوامل، منها

- ازدياد اعتماد الجهات الحكومية على التكنولوجيا الرقمية في تقديم الخدمات للجمهور.
- تطوير تقنيات الهجمات السيبرانية وزيادة تعقيدها.
- تزايد نشاط الجماعات والجهات الممولة من الخارج التي تستهدف البنية التحتية الرقمية للدول.

13. ما هي الثغرات الأمنية الأكثر استغلالاً في نظام الحكومة الرقمية في الامارات؟ وما هي التدابير المتخذة لسد هذه الثغرات؟

تشمل الثغرات الأمنية الأكثر استغلالاً في نظام الحكومة الرقمية في الامارات ما يلي:

- عدم تحديث أنظمة التشغيل والبرامج المستخدمة في الخدمات الحكومية.
- ضعف الوعي الأمني لدى المستخدمين الحكوميين.
- عدم وجود أنظمة حماية فعالة لاكتشاف ومنع الهجمات السيبرانية.

وتشمل التدابير المتخذة لسد هذه الثغرات ما يلي:

- تنفيذ برامج تحديث مستمر لأنظمة التشغيل والبرامج المستخدمة في الخدمات الحكومية.
- إطلاق حملات توعية أمنية للمستخدمين الحكوميين لرفع مستوي الوعي لديهم بالمخاطر السيبرانية.
- تطوير أنظمة حماية فعالة لاكتشاف ومنع الهجمات السيبرانية.

14. كيف يتم تصنيف وتقييم الأولويات في مجال الأمن السيبراني للخدمات الحكومية الرقمية في الامارات؟

تم تصنيف وتقييم الأولويات في مجال الأمن السيبراني للخدمات الحكومية الرقمية في الامارات بناء على عدة عوامل، منها

- مستوى المخاطر السيبرانية التي تواجه الخدمات الحكومية.
- أهمية الخدمات الحكومية التي يتم استهدافها.
- تكلفة وفعالية الإجراءات الأمنية التي يمكن اتخاذها.

وتهدف هذه الإجراءات إلى تعزيز الأمن السيبراني للخدمات الحكومية الرقمية في الامارات وحماية البيانات والمعلومات الحساسة من الهجمات السيبرانية.

محور: أثار التهديدات السيبرانية على الخدمات الحكومية الرقمية في الامارات

15. ما هي الآثار السلبية المتوقعة للاختراقات السيبرانية على الخدمات الحكومية الرقمية في الامارات؟

يمكن أن تؤدي الاختراقات السيبرانية إلى مجموعة متنوعة من الآثار السلبية على الخدمات الحكومية الرقمية في الامارات، بما في ذلك

- **تعطل الخدمات:** يمكن أن يؤدي الاختراق إلى تعطل الخدمات الحكومية الرقمية بشكل كامل أو جزئي، مما يتسبب في عدم إمكانية الوصول إليها من قبل المواطنين والشركات.
- **فقدان البيانات:** يمكن أن يؤدي الاختراق إلى سرقة أو فقدان البيانات الحكومية الحساسة، مما قد يعرض أمن البلاد وسلامة مواطنيها للخطر.
- **الضرر المالي:** يمكن أن تؤدي الهجمات السيبرانية إلى إلحاق ضرر مالي بالحكومة، على سبيل المثال من خلال دفع فدية أو اصلاح الاضرار الناجمة عن الهجوم.

16. كيف يؤثر انقطاع الخدمات الحكومية الرقمية بسبب هجمات سيبرانية على المواطنين والشركات في الامارات؟

يمكن أن يؤثر انقطاع الخدمات الحكومية الرقمية بسبب هجمات سيبرانية على المواطنين والشركات في الامارات بطرق مختلفة، بما في ذلك:

- **عدم القدرة على الوصول إلى الخدمات الأساسية:** يمكن أن يؤدي انقطاع الخدمات الحكومية الرقمية إلى عدم القدرة على الوصول إلى الخدمات الأساسية، مثل الخدمات الصحية والتعليمية والمالية.
- **عرقلة الاعمال التجارية:** يمكن أن يؤدي انقطاع الخدمات الحكومية الرقمية إلى تعطيل في الأعمال التجارية، مما يؤثر على الأرباح وانتاجية العمال.
- **صعوبة أنجاز المهام اليومية:** يمكن أن يؤدي انقطاع الخدمات الحكومية الرقمية إلى صعوبة إنجاز المهام اليومية، مثل دفع الفواتير أو حجز موعد مع الطبيب.

17. ماهي التكاليف المحتملة لاستعادة وإصلاح الأضرار الناتجة عن الهجمات السيبرانية على البنية التحتية الحكومة الرقمية في الامارات؟

يمكن أن تكون التكاليف المحتملة للاستعادة وإصلاح الأضرار الناتجة عن الهجمات السيبرانية على البنية التحتية الحكومة الرقمية في الامارات باهظة للغاية، وقد تصل إلى ملايين أو حتى مليارات الدراهم وتعتمد هذه التكاليف على عدة عوامل، بما في ذلك حجم الهجوم، ومدى انتشاره، ونوع الأضرار التي لحقت بالأنظمة والبيانات.

بشكل عام، يمكن تقسيم التكاليف المحتملة لاستعادة والإصلاح إلى ثلاث فئات رئيسية

- **التكاليف المباشرة:** تتضمن هذه التكاليف تكلفة استعادة الأنظمة والبيانات التي تم تعطيلها أو اتلافها نتيجة للهجوم. قد تشمل هذه التكليف تكلفة استعادة نسخة احتياطية من البيانات، أو إعادة تثبيت البرامج والأنظمة، أو اصلاح البنية التحتية المتضررة.
- **التكاليف الغير مباشرة:** تتضمن هذه التكاليف الخسائر الاقتصادية الناجمة عن الهجوم، مثل انخفاض الإنتاجية، أو فقدان ثقة المستثمرين.

18. هل يمكن استعادة البيانات المسروقة أو التالفة نتيجة للاختراقات السيبرانية في الامارات؟ وماهي التدابير المتبعة لذلك؟

في بعض الحالات، يمكن استعادة البيانات المسروقة أو التالفة نتيجة للاختراقات السيبرانية في الامارات. ومع ذلك، فإن ذلك يعتمد على مدى تعقيد الهجوم، ومدى توفر نسخة احتياطية من البيانات

وهناك عدد من التدابير التي يمكن اتخاذها لزيادة فرص استعادة البيانات المسروقة أو التالفة، وبما في ذلك:

الاحتفاظ بنسخة احتياطية من البيانات بشكل دوري: يجب أن تتضمن نسخة الاحتياط

جميع البيانات المهمة ويجب أن يتم تخزينها في موقع آمن بعيد عن الشبكة.

- **استخدام تقنيات التشفير:** يمكن استخدام تقنيات التشفير للحماية من سرقة البيانات، حيث يمكن فك تشفير البيانات فقط باستخدام مفتاح خاص.
- **رفع كفاءة الموظفين:** من خلال التدريب على الأمن السيبراني وعقد تمارين سيبرانية، لزيادة وعيهم بالمخاطر السيبرانية وكيفية التصدي لها.
- **تنفيذ سياسات وإجراءات الأمن السيبراني:** تساعد سياسات وإجراءات الأمن السيبراني على حماية البيانات من المخاطر المختلفة، بما في ذلك التهديدات السيبرانية.

19. ما هي تأثير الهجمات السيبرانية على سمعة الامارات وموثوقيتها في مجال الخدمات الحكومية الرقمية؟

تتمتع الامارات العربية المتحدة بسمعة طيبة في مجال الخدمات الحكومية الرقمية، حيث تعتبر من الدول الرائدة في هذا المجال وقد ساهمت هذه السمعة في جذب الاستثمارات الأجنبية وتعزيز الاقتصاد الوطني ومع ذلك، فإن الهجمات السيبرانية يمكن أن تؤثر سلباً على سمعة الامارات وموثوقيتها في مجال الخدمات الحكومية الرقمية. فعندما تتعرض الخدمات الحكومية الرقمية لهجمات سيبرانية، فأن ذلك يؤدي إلى تعطلها أو اختراقها، مما قد يسبب في حدوث خسائر مالية أو أمنية.

محور: الطرق والممارسات الناجحة للتعامل مع التهديدات

20. ما هي أفضل الممارسات والإجراءات التي يجب اتباعها للوقاية من التهديدات السيبرانية على الخدمات الحكومية الرقمية في الامارات؟

تتمثل أفضل الممارسات والإجراءات التي يجب اتباعها للوقاية من التهديدات السيبرانية على الخدمات الحكومية الرقمية في الامارات

- اتباع السياسات والمعايير الوطنية للأمن السيبراني، بما في ذلك الإطار الوطني لضمان أمن المعلومات وسياسات مجلي الأمن السيبراني والتي تتضمن في مرحلتها الأولي:

◊ إطار حوكمة الأمن السيبراني الوطني.

◊ سياسة حماية البنية التحتية للمعلومات الحيوية.

◊ سياسة أمن السحابة.

◊ سياسة أمن أنترنت الأشياء.

◊ الخطة الوطنية للاستجابة للحوادث.

◊ إطار عمل مشاركة المعلومات.

◊ القدرات الأساسية لمركز العمليات الأمني السيبراني.

◊ برنامج الاعتماد الخاص بالأمن السيبراني.

أتباع أفضل الممارسات الأمنية في مجال تطوير وإدارة الخدمات الحكومية الرقمية، بما في ذلك

◊ استخدام تقنية الأمن المناسبة، مثل التشفير وإدارة الهوية، وإدارة وصول المستخدمين.

◊ إجراء تقييمات الأمان الدورية لتحديد نقاط الضعف المحتملة.

◊ نشر التحديثات الأمنية في الوقت المناسب.

الاستثمار في التدريب وتوعية الموظفين الحكوميين حول الأمن السيبراني، بما في ذلك

◊ تعليم الموظفين حول كيفية التعرف على التهديدات السيبرانية وكيفية حماية أنفسهم منها.

◊ تدريب الموظفين على كيفية التعامل مع الحوادث السيبرانية.

◊ التعاون مع الجهات الحكومية الأخرى والمؤسسات الخاصة لتبادل المعلومات حول التهديدات السيبرانية وأفضل الممارسات الأمنية.

21. كيف يمكن تعزيز قدرة الحكومة الإماراتية على الكشف المبكر عن التهديدات السيبرانية والتصدي لها؟

يمكن تعزيز قدرة الحكومة الإماراتية على الكشف المبكر عن التهديدات السيبرانية والتصدي لها من خلال ما يلي

- تفعيل مركز العمليات الأمني الوطني COSN ف كافة الجهات العاملة في الدولة، والذي يعمل على رصد التهديدات السيبرانية والتصدي لها باستباقية وفاعلية باستخدام أحدث التقنيات والتكنولوجيا.
- استخدام تقنيات الذكاء الاصطناعي لتحليل البيانات واكتشاف التهديدات المحتملة.
- التعاون مع الجهات الحكومية الأخرى والمؤسسات الخاصة لتبادل المعلومات حول التهديدات السيبرانية.

22. ما هي دور التدريب والتوعية في تعزيز الأمن السيبراني للخدامات الحكومية؟

يلعب التدريب والتوعية دوراً اساسياً في تعزيز الأمن السيبراني للخدمات الحكومية، وذلك من خلال ما يلي

- الاستمرار في عقد تمارين تحاكي الهجمات السيبرانية لرفع كفاءة موظفي أمن المعلومات في مختلف مؤسسات الدولة.
- تطوير وتنفيذ استراتيجية شاملة للأمن السيبراني للخدمات الحكومية، تستند إلى أفضل الممارسات العالمية.
- زيادة الاستثمار في مجال الأمن السيبراني، بما في ذلك التدريب والتوعية والبنية التحتية الأمنية.

- التعاون مع الجهات الحكومية الأخرى والمؤسسات الخاصة لتبادل المعلومات والقدرات.

محور: التطوير المستمر في منظومة الأمن السيبراني والتوعية:

23. ما هي الجهود التي تبذلها الامارات لتطوير منظومة الأمن السيبراني للحكومة الرقمية؟

تبذل دولة الامارات جهوداً كبيرة لتطوير منظومة الأمن السيبراني للحكومة الرقمية، وذلك من خلال التركيز على المحاور التالية

- **البنية التحتية الأمنية:** تسعى دولة الامارات إلى تطوير بنية تحتية أمنية قوية وحديثة، وذلك من خلال تحديث الأنظمة الأمنية وتطبيق أفضل الممارسات العالمية، وتعزيز التعاون الدولي في مجال الأمن السيبراني.
- **القدرات البشرية:** تعمل دولة الامارات على بناء قدرات بشرية مؤهلة في مجال الأمن السيبراني، وذلك من خلال تقديم برامج تدريبية متخصصة بما يشمل مبادرات رائدة كمبادرة القناص السيبراني ومبادرة الدرع الواقي السيبراني، وبالإضافة إلى عقد الشراكات مع مؤسسات عالمية رائدة في هذا المجال.
- **التوعية المجتمعية:** تحرص دولة الامارات على نشر الوعي بالأمن السيبراني بين أفراد المجتمع، وذلك من خلال إطلاق حملات توعوية مكثفة، وتوفير قنوات إلكترونية ومطبوعة لنشر المعلومات حول الأمن السيبراني وذلك من خلال العديد من المبادرات نذكر منها، مبادرة النبض السيبراني ومبادرة قادة المستقبل في الأمن السيبراني، إضافة بالخطة الوطنية للتوعية السيبرانية وتشمل حملات توعوية أسبوعية على مدار السنة.

24. كيف يتم تحديث استراتيجيات الأمن السيبراني في الامارات لمواجهة التهديدات المتطورة؟

يتم تحديث استراتيجيات الأمن السيبراني في الامارات لمواجهة التهديدات المتطورة من خلال مجموعة من الإجراءات والعمليات، منها

- **الرصد المستمر للتهديدات السيبرانية:** تقوم الجهات المختصة في الامارات برصد مستمر للتهديدات السيبرانية الجديدة والتطورات في الأساليب الهجومية، وذلك من خلال التعاون مع الجهات الدولية والإقليمية، واستخدام أحدث التقنيات والأدوات التحليلية.
- **التحليل الاستباقي للمخاطر:** تقوم الجهات المختصة بتحليل المخاطر السيبرانية المحتملة، وذلك من خلال دراسة التهديدات الحالية والمستقبلية، وتحديد نقاط الضعف في الأنظمة والشبكات.
- **التطوير المستمر للقدرات الأمنية:** تقوم الجهات المختصة بتطوير قدراتها الأمنية باستمرار، وذلك من خلال الاستثمار في التدريب والتأهيل، واستخدام أحدث التقنيات والحلول الأمنية.

25. ما هي أهم الابتكارات التقنية المستخدمة في مجال الأمن السيبراني للحكومة الرقمية في الامارات؟

تستخدم الامارات العديد من الابتكارات التقنية في مجال الأمن السيبراني للحكومة الرقمية، ومن أهم هذه الابتكارات هي تقنية الذكاء الاصطناعي (IA)، والتي تستخدم في تحليل البيانات واكتشاف التهديدات السيبرانية المحتملة

26. كيف يتم توعية الموظفين والجمهور بأهمية الأمن السيبراني وكيفية التصدي للتهديدات السيبرانية في الامارات؟

ضمن محور التطوير المستمر في منظومة الأمن السيبراني والتوعية، يتم توعية الموظفين والجمهور بأهمية الأمن السيبراني وكيفية التصدي للتهديدات السيبرانية في الامارات من خلال مجموعة من المبادرات والبرامج، منها:

- **إطلاق حملات توعوية وطنية وإقليمية وعالمية:** تقوم الجهات المعنية في دولة الامارات بإطلاق حملات وطنية وإقليمية وعالمية حول أهمية الأمن السيبراني وكيفية حماية البيانات والمعلومات من التهديدات السيبرانية، وتشمل هذه الحملات مجموعة متنوعة من الوسائل، مثل الإعلانات التلفزيونية والاذاعية والمطبوعة، والندوات والمؤتمرات، البرامج التعليمية الإلكترونية.
- **تطوير برامج تطويرية متخصصة:** توفر الجهات المعنية في دولة الامارات برامج تدريبية متخصصة حول الأمن السيبراني للموظفين والجمهور، وتهدف هذه البرامج إلى تزويد المشاركين بالمهارات والخبرات اللازمة لفهم التهديدات السيبرانية وكيفية مواجهتها.
- **إدراج موضوعات الأمن السيبراني في المناهج الدراسية:** يتم إدراج موضوعات الأمن السيبراني في المناهج الدراسية في دولة الامارات، وذلك بهدف تعزيز الوعي الأمني لدى الطلاب منذ سن مبكرة.

27. ماهي الشراكات المحلية والدولية التي تساهم في تطوير منظومة الأمن السيبراني للحكومة الإماراتية؟

تحرص دولة الامارات على التعاون مع الجهات المحلية والدولية في مجال الأمن السيبراني، وذلك من خلال المشاركة في المؤتمرات والندوات الدولية، وتوقيع الاتفاقيات الثنائية والمتعددة الأطراف، ومن أهم هذه الشراكات

- الشراكة مع الاتحاد الدولي للاتصالات، والتي تهدف إلى تعزيز التعاون في مجال الأمن السيبراني.
- الشراكة مع شركات عالمية بما يشمل شركة سيسكو، والتي تهدف إلى تطوير قدرات الأمن السيبراني في الدولة.
- التعاون مع الدول العربية والمنظمات الإقليمية، والتي تهدف إلى تعزيز التعاون

الإقليمي والدولي في مجال الأمن السيبراني.

- المشاركة في اللجان الخليجية والإقليمية والدولية والتي تهدف إلى تبادل الخبرات والمعرفة في الأمن السيبراني، وذلك بما يتضمن المبادرة الدولية لمكافحة برامج فدية (CRI) حيث تترأس الدولة إحدى اللجان الرئيسية في المبادرة، إضافة إلى اللجنة الوزارية للأمن السيبراني لدول مجلس التعاون ومنظمة التعاون الإسلامي للاستجابة للطوارئ الحاسوبية (OIC-CERT) حيث انتخبت دولة الامارات نائباً للرئيس في فريق منظمة التعاون الإسلامي للاستجابة لحوادث الطوارئ الحاسوبية.


تم بحمد الله