أمن المعلومات الرقمية وسُبل حمايتها في ظل التشريعات الراهنة

أ د. عزة فاروق عبد المعبود جوهري

أ. طه محمد طه حسن

قسم علوم المعلومات – كلية الآداب – جامعة بني سويف

مستخلص:

ساهم التطور التكنولوجي في مجال الاتصالات وتقنيات المعلومات في سرعة انتشار المعلومات وسهولة تداولها عبر خدمات الإنترنت مما أدى إلى ظهور العديد من المخاطر والاعتداءات التي تتم في بيئة الإنترنت الأمر الذي أدى إلى ضرورة نشر الوعي بين المستخدمين لحماية أمن المعلومات، وذلك من خلال قيام العديد من الدول إلى وضع التشريعات التي تحمي أمن المعلومات فضلاً عن العديد من المنظمات التي تقوم بوضع مواصفات دولية لتكون بمثابة الدليل الاسترشادي الأمثل لحماية أمن المعلومات مثل منظمة الأيزو.

تهدف الدراسة الحالية إلى التعرف على المخاطر التي يتعرض لها أمن المعلومات الرقمية بأشكالها المختلفة والتدابير المضادة للحد من هذه المخاطر مثل التدابير التنظيمية والمادية والتقنية بالإضافة إلى التدابير التشريعية على المستويين الوطني والدولي وأهم المعايير الدولية التي تضعها منظمة الأيزو لضبط ممارسات أمن المعلومات.

وتوصلت الدراسة إلى عدة نتائج أهمها أن أمن المعلومات يتعرض للعديد من المخاطر والتهديدات التي تتم في بيئة الإنترنت مع صعوبة مواكبة التدابير الأمنية المضادة لسرعة تطور الأساليب الحديثة المستخدمة في عمليات الاعتداءات على أمن المعلومات، ضعف التشريعات الموجودة على أرض الواقع سواء على المستوى الوطني أو الدولي مع وجود بطء ملحوظ في مدى كفاية التشريعات الموجودة للحد من عمليات التعدي على أمن المعلومات.

الكلمات المفتاحية: أمن المعلومات، مخاطر أمن المعلومات، المعايير الدولية لأمن المعلومات، تشريعات أمن المعلومات.

Abstract:

The development of technology in the field of communication and information technology play an important part in the spread of information via the internet. Attacks and risks are vulnerable to this environment where users are a warned against these risks to protect and save their information. For many reasons, many countries have established legislation that protects information security as well as many organizations set international standards to serve as the best guide for information security protection such as ISO.

The present study investigates digital information security with all its shapes and types and establishes legislation to protect users against all risks such as organizational, financial, and technical measures in addition to legislative measures on the local and international level and the most important established international standards by ISO to control information security practices.

The study found several findings, the most important of which is that Information Security is exposed to many of the risks and threats that occur in the Internet environment with the difficulty of keeping pace with security measures against the speed of development of modern methods and techniques used in these attacks. Indeed, weak existing legislations on the local and international level and adequacy of existing legislation do not limit information security attacks.

Keywords: Information Security, Information Security Risks, International Measures of Information Security, Information security legislation.

التمهيد:

إن العصر الذي نعيش فيه أصبح عصرًا معلوماتيًا بكل ما تحمله الكلمة من معنى في ظل الثورة التكنولوجية الهائلة التي طرأت على المجتمع، فأصبحت المعلومات هي الركيزة الأساسية التي يعتمد عليها في كل مناحي الحياة، وذلك في ظل التقنيات الحديثة ووسائلها المتعددة التي اخترعت لتسهل أمور الحياة على الإنسان حتى أنها أصبحت تقوم ببعض وظائفه في العديد من المجالات.

ونتيجة لانتشار شبكة الإنترنت فقد أشارت العديد من الدراسات الحديثة أن نسبة مستخدمي الإنترنت تتزايد باستمرار فقد وصل عدد مستخدمي الإنترنت على مستوى العالم في إحصاء 2018 إلى 4.208 مليار[1]، وعلى مستوى العالم العربي بلغ العدد الكلي لمستخدمي الإنترنت إلى 185 مليون مستخدم وتحتل مصر من بين الدول العربية المرتبة الأولى بعدد 50 مليون مستخدم للإنترنت[2]، ومع تزايد أعداد مستخدمي خدمات الإنترنت تتزايد الاستخدامات وبالتالي تتبادل المعلومات والبيانات بشتى أنواعها على مستوى العالم وتتنوع معها أهمية هذه المعلومات ودرجة سريتها وقيمتها الاقتصادية والمعنوية بين الدول والهيئات أو المؤسسات وكذلك الأفراد.

ومع توسع استخدام خدمات الإنترنت وانتشار استخدامه وخاصة مع ظهور التجارة الإلكترونية والحكومات الإلكترونية واعتماد الدول ذات القيمة الاقتصادية الكبرى على خدمات الإنترنت في نواحي كثيرة ظهر الجانب السلبي لاستخدام الإنترنت بظهور أنماط جديدة من الجرائم المستحدثة على هذه الخدمة وهو ما يطلق عليه الجرائم المعلوماتية وما تشمله من أعمال القرصنة والتجسس وانتهاك خصوصيات الغير وجرائم سرقات المعلومات.

لذلك كانت هناك حاجة ماسة إلى تعاون دولي للحد من الجرائم الإلكترونية وحماية أمن المعلومات عن طريق تبادل الخبرات والتعاون على إيجاد وسائل قانونية

وتقنية لمواجهة الأخطار التي تهدد أمن المعلومات مع الأخذ في الاعتبار الطبيعة المختلفة لبلدان العالم، واللغات الموجودة على شبكات الإنترنت.

مشكلة الدراسة:

بدأ التركيز على شبكات الإنترنت كتهديد أمني جديد بفعل الأحداث الدولية التي ظهرت نتيجة الانتهاكات التي تتم عبر خدمات الإنترنت وأبرزها أحداث 11 سبتمبر 2001 في الولايات المتحدة الأمريكية ثم في عام 2010 حين تم الهجوم الإلكتروني على برنامج إيران النووي عن طريق فيروس يسمى (ستاكسنت) ليمثل نقلة هامة بالتطور في مجال الأسلحة الإلكترونية، بالإضافة إلى الدور السياسي الذي لعبته مواقع التواصل الاجتماعي فيما يسمى بثورات الربيع العربي في بداية عام 2011[3]، بالإضافة إلى ما أعلنته شركة ياهوو Yahoo الشهيرة في عام 2016 أن أكثر من بليون حساب على سيرفراتها جرت عليه عمليات القرصنة وسرقة بيانات المستخدمين من أسماء وأرقاهم هواتف لشخصيات عامة وعالمية[4].

أدت هذه الجرائم إلى خسائر مالية فادحة يتكبدها الإقتصاد العالمي سنويًا بحسب تقرير أصدره مركز الدراسات الإستراتيجية بواشنطن بالتعاون مع شركة مكافي MacAfee لبرامج الأمن المعلوماتي لعام 2018، أن الإقتصاد العالمي يتكلف نحو 600 مليار دولار خسائر سنويًا أي بما يعادل نحو 1% من الدخل الإجمالي العالمي بسبب جرائم الإنترنت، مقارنة بحجم الخسائر لعام 2014 المقدرة بحوالي 500 مليار دولار أي بارتفاع وصلت نسبته إلى 0.8%[5].

أشار Grant Gross جرانت جروس في التعليق على التقرير السابق أنه بجانب الخسائر الاقتصادية فإنه هناك ما يقدر بنحو 80 مليون من المسح الإلكتروني للبحث عن الثغرات الموجودة في أجهزة مستخدمي شبكة الإنترنت يوميًا، بالإضافة إلى 780.000 عملية سرقة للحسابات الشخصية[6].

لذلك فقد تجسدت مشكلة الدراسة في رصد المخاطر التي تحيط بأمن المعلومات الرقمية والتدابير الأمنية التي يجب توافرها ومعرفة ما يتوافر من تشريعات بهذا الصدد من جهود محلية ودولية وعالمية.

أهمية الدراسة:

تظهر أهمية دراسة أمن المعلومات بشكل خاص في أن معلومة ما قد تحمل اكتشاف جديد يفيد البشرية في مجال ما، ومعلومة أخرى تتعلق بالاقتصاد تكون سببًا في إفلاس دول اقتصاديًا وأخرى تساعد في بناء اقتصادها، لذا فإن أهمية المعلومة تظهر في ابتكارها وإحسان استخدامها، وإذا ما أردنا تحديد الأهمية المادية للمعلومة نجد أن علماء أمن المعلومات انقسموا إلى اتجاهين لتحديد أهميتها[7]:

الاتجاه التقليدي: الاتجاه الذي لا يرى في المعلومات أي قيمة مادية بل أنها ذات طبيعة معنوية لا تندرج تحت القيم المحمية، إلا إذا كانت تنتمي إلى المصنفات الأدبية والفنية أو الصناعية.

الاتجاه الحديث: يرى أن للمعلومات قيمة مالية أشبه بالسلعة، فهي نتاج ذهني ولكي تكون صالحه للتملك لا بد وأن يحوز مالكها على العناصر المكونة لها بطريقة شرعية في قالب يصلح للاطلاع عليها بغض النظر عن الوسيط الذي يتضمنها.

من هنا كان الاهتمام بهذه الدراسة لمعرفة الضوابط التي تحول دون انتهاك قيمة المعلومات والتدابير الأمنية المتوافرة لحمايتها وضمان وصولها بطريقة شرعية.

أهداف الدراسة:

في ضوء مشكلة وأهمية الدراسة، فإن هذه الدراسة تسعى إلى تحقيق عدد من الأهداف التي يمكن إيجازها في النقاط التالية:

1. التعرف على مفهوم أمن المعلومات وعناصره

2. التعرف على المخاطر التي تهدد أمن المعلومات.
3. التعرف على أساليب مواجهة الاعتداءات التي تواجه أمن المعلومات.
4. الوقوف على أحدث التشريعات الراهنة ومدى كفايتها لحماية أمن المعلومات.
5. أهم المعايير الدولية الخاصة بحماية أمن المعلومات.

منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي وذلك من خلال الاستعانة بالمصادر العلمية ذات العلاقة بأمن المعلومات، وما توافر من الإنتاج الفكري.

مصطلحات الدراسة:

أمن المعلومات Information Security:

عبارة عن مجموعة العمليات أو المعايير والآليات التي تُصمم وتُنفذ لأغراض حماية المعلومات من الوصول غير المشروع من أجل إساءة الاستخدام أو التخريب[8]، ويكون ذلك من أجل ضمانة وسلامة المعلومات، في هذا السياق نجد أن مصطلح أمن المعلومات هو مصطلح عام يمكن أن ينطبق على أي شكل من أشكال المعلومات سواء كانت تقليدية أو رقمية.

التشريعات Legislations:

هي مجموعة القواعد المكتوبة التي تنظم العلاقة القائمة بين الأطراف المعنية والداخلة فيه. ولهذه القواعد القوة الجبرية اللازمة للتنفيذ والتقيد بها، والعقاب في حالة المخالفة؛ ولكي تكون القواعد تشريعًا فلابد وأن تكون مكتوبة استناداً إلى القاعدة التشريعية التي تقول بأنه لا عقوبة إلا بنص[9].

المحتوى الرقمي Digital Content:

عبارة عن المواقع الإلكترونية المكتوبة (المبنية والمرفوعة) بإحدى لغات التكويد الخاصة بتحويل النص التناظري إلى نص رقمي[10]، والكيانات الرقمية التي تعد شكل جديد من أشكال أوعية المعلومات الرقمية، تحتوي على ملف رقمي واحد أو أكثر من ملف من أشكال الملفات الرقمية[11].

المصنفات الرقمية Digital Works:

هي الشكل الرقمي لمصنفات موجودة ومعدة سلفاً دون تغيير أو تعديل في النسخة الأصلية للمصنف سابق الوجود، كأن يتم نقل النص المكتوب (مصنف أدبي) أو الصوت (مصنف سمعي)، أو الصوت والصورة معا (مصنف سمعي بصري) من الوسيط التقليدي الذي كان عليه إلى وسيط تقني رقمي متطور كالأقراص المدمجة CD-ROM أو الأسطوانات المدمجة الرقمية DVD وهي الشكل الرقمي منذ البدء لأي مصنف، بحيث يكون التثبيت المادي الأول للمصنف وعمل نسخ منه تم على وسط تقني متطور[12].

الدراسات السابقة:

اهتمت العديد من الدراسات العربية والأجنبية بموضوع أمن المعلومات في بيئة الإنترنت والتشريعات المختصة بحمايته باعتباره موضوع ذا طبيعة خاصة جديرة بالاهتمام والبحث، ومن أهم الدراسات التي تناولت هذا الموضوع ما يلي:

1 - الدراسات العربية:

هدفت دراسة إيهاب نور الدين في عام 2018[13]، إلى قياس وتفسير أثر الإسناد الخارجي لمهام تكنولوجيا المعلومات على أمن وسرية المعلومات وذلك من خلال تحقيق عدة أهداف فرعية كان أهمها القيام بدراسة تحليلية لقياس وتفسير أثر هذا

الإسناد والتعرف على مزاياه وعيوبه من خلال استخدام المنهج الاستقرائي عن طريق تصميم قائمة استقصاء وتوزيعها على المتخصصين في مجال تكنولوجيا المعلومات.

واقتصرت الدراسة على بيان مدى تأثير الإسناد الخارجي لمهام تكنولوجيا المعلومات دون التطرق إلى دور هذا الإسناد تقديم خدمات استشارية أخرى، عن طريق عينه من داخل حدود البيئة المصرية تشتمل على مجموعتين: الأولى مكونة من المهندسين في مجال تكنولوجيا المعلومات ومجموعة أخرى خاصة بالمهندسين الذين يقدمون خدمة الإسناد الخارجي.

وخلصت الدراسة من خلال تحليل نتائج الاستقصاء على العينة المذكورة إلى أنه توجد علاقة ارتباط بين الإسناد الخارجي لمهام تكنولوجيا المعلومات وأمن وسرية المعلومات.

أما دراسة عبد الوهاب ملياني عام 2017[14]، سعت إلى تحليل ظاهرة الجرائم الواقعة على النظام المعلوماتي باعتباره البيئة التي تتم فيها كل الأعمال الخاصة بالمعلومات الإلكترونية من خلال القيام بدراسة تأصيلية لتلك الجرائم باعتبارها سبباً أصيلاً لصدور التشريعات الخاصة بحماية أمنها، متبِعاً في ذلك المنهج الوصفي التاريخي والمنهج المقارن بالإضافة إلى المنهج الاستدلالي.

وقام الباحث بدراسة المعالجة التشريعية لأمن المعلومات الرقمية وتحديد طبيعة الجرائم التي ترتكب عليها وتحديد مدى استقلاليتها عن غيرها من الجرائم وما ينعكس بذلك على النصوص التشريعية في المجال الجنائي مع الوقوف على مدى توفيق المشرع في وضع استراتيجية لمواجهة تلك الجرائم على الجانبين الموضوعي والإجرائي.

توصلت الدراسة إلى العديد من النتائج أهمها ضرورة أن تتضمن مقومات استراتيجيات مواجهة جرائم الاعتداء ومحاربتها على الجوانب الجنائية الموضوعية

والإجرائية تتماشى وطبيعة البيئة الرقمية حيث إنها لا تكفي وحدها لمواجهة الجرائم محل الدراسة ولابد من إيجاد استراتيجيات مكملة على المستوى الفني والتقني والقضائي وضرورة التعاون القضائي الدولي في مسألة تسليم المجرمين.

سعى الباحث معاذ أحمد عبد الرازق في عام 2016[15]، إلى التعرف على المهددات التي تتعرض لها المعلومات ومحاولة التوصل إلى مقترحات تساهم في التصدي لها والأنظمة الكفيلة بالحد من تلك الظواهر السلبية بالإضافة إلى التعرف على وسائل حماية المعلومات والبيانات.

اتبع الباحث في تحقيق أهدافة من الدراسة المنهج الوصفي التحليلي وعمل مسح للمركز القومي للمعلومات عن طريق الاستبانة وإجراء المقابلات الشخصية والزيارات الميدانية والملاحظات ونتيجة لذلك توصل الباحث في نهاية الدراسة إلى عدد من النتائج أهمها استخدام أنظمة الحماية والمعايير العالمية لأمن المعلومات هي من أنسب الطرق التي يمكن اتباعها للحد من المخاطر التي تهدد أمن المعلومات، أوصت الدراسة بإنشاء وحدة تهتم بأمن المعلومات في كافة مرافق الدولة وضرورة التوعية وعمل تدريبات دورية للمستخدمين على أحدث الأنظمة والتقنيات المستخدمة في مجالات أمن المعلومات.

أما الباحثة منال بنت حمدان في عام 2016[16]، قد سعت إلى الكشف عن ممارسات أمن المعلومات المتبعة في المكتبة الرئيسية بجامعة السلطان قابوس للوقوف على مدى توافقها مع المعيار الدولي لأمن المعلومات (ISO/IEC 27002) من أجل معرفة نقاط الضعف والقوة التي قد تؤدي إلى تحسين الممارسات الأمنية بالمكتبة الرئيسية بدولة عمان.

اعتمدت الباحثة في دراستها على منهج دراسة الحالة من خلال استخدام عدة أساليب مثل الزيارات الميدانية والمقابلات الشخصية واستخدام أداة لجمع

البيانات لفئة العاملين في الأقسام المسئولة عن ممارسات أمن المعلومات بجامعة السلطان قابوس استهدفت منهم رؤساء الأقسام ومن ينوب عنهم في كل قسم.

وخلصت الدراسة إلى أن أغلب ممارسات أمن المعلومات بالمكتبة تتوافق مع ممارسات المعيار الدولي لأمن المعلومات (ISO/IEC 27002)، ونتيجة لهذه النتيجة فقد وضعت الباحثة عدة توصيات أهمها ضرورة تدريب وتوعية المستفيدين من المكتبات وتطوير سياسات أمن المعلومات بالمكتبات مستندة على المعيار الدولي لأمن المعلومات، مع ضرورة توفير التدابير المادية اللازمة مثل النسخ الاحتياطي وتوفير مصادر بديلة للطاقة.

2 - الدراسات الأجنبية:

هدفت الباحثة Venessa Burton في دراستها عام 2018[17]، إلى التعرف على التحديات التي يواجها مدراء أمن المعلومات في بيئة الإنترنت المتخصصين في حماية المعلومات التجارية ومحاولة معرفة مدى كفاية حماية الملكية الفكرية من الانتهاكات التي يرتكبها مجرمي الإنترنت، وتأثير ذلك على مسئولي الأمن المعلوماتي، وقامت الباحثة بدراسة قدرة هؤلاء المديرين على تطبيق قوانين حماية الملكية الفكرية على حماية أصول منشآت الأمن المعلوماتي ودراسة المخاطر التي تتعرض لها وذلك من خلال التعرف على الاستراتيجيات التي يتم استخدامها في تطبيق الحماية القانونية وآلية حمايتها ضد الإرهاب الإلكتروني.

استندت الباحثة في تحقيق أهدافها على البحث النوعي من خلال إجراء المقابلة الشخصية لعشرة مديرين من المتخصصين في مجال أمن المعلومات ولهم سنوات خبرة في هذا المجال لا تقل عن 15 سنة من التعامل مع الشبكات والبنية التحتية لأمن المعلومات وفي مدينة واشنطن بالولايات المتحدة الأمريكية.

وخلصت الدراسة إلى أن القوانين المتبعة في حماية أمن المعلومات في بيئة الإنترنت تبطئ من عمل المديرين في أمن المعلومات نظراً لعدم مواكبتها للجرائم الحديثة لذلك فهي ليست فعالة بالشكل الكافي، كما أن القوانين تفتقر إلى آلية واضحة للتطبيق نظراً لتشعب وتنوع الجرائم الإلكترونية، لذلك أوصت الباحثة أنه لابد من توحيد القوانين التي تتصدى لهذه الجرائم بالإضافة إلى وضع سياسات واستراتيجيات لأمن المعلومات تكون كافية لتنظيم ممارسات الأمن والحماية.

تناولت دراسة Ghafir Ibrahim في عام 2018[18]، الجانب المعرفي لدى العاملين والمستخدمين لأمن المعلومات في بيئة الإنترنت على وجه الخصوص، وما يترتب على الوعي الأمني لديهم من مخاطر تتمثل في إمكانية حدوث جرائم الاحتيال والجرائم التي تتم باستخدام الهندسة الاجتماعية عندما يتم تسجيل دخول المستخدم للوصول إلى المواقع الإلكترونية، والتدابير التي يمكن تنفيذها لحماية البيانات الشخصية والتجارية من الخسارة المحتملة.

وتوصلت الدراسة إلى تطوير برنامج تدريبي لزيادة الوعي الأمني لمساعدة الشركات والعاملين فيها لمعرفة المخاطر الإلكترونية المحتملة لحماية أنفسهم والمكان الذي يعملون فيه، ويوفر أيضاً البرنامج التدريبي التحديثات المستمرة لأهم الجرائم التي تتم في البيئة الرقمية مع التدريب على التدابير الأمنية للتصدي لهذه الجرائم، مع إمكانية إصدار شهادات عند النجاح في جميع الوحدات المكونة للبرنامج التدريبي.

أما الباحث Michele Zoerb فقد قام بدراسة عام 2017[19]، تهدف إلى وضع إطار عام لمفهوم أمن المعلومات في بيئة الإنترنت نظراً لملاحظته وجود تفاوت بين مفهوم أمن المعلومات وسياسات أمن المعلومات والضوابط الداخلية لمنظمات أمن المعلومات، وهذا التفاوت في التعريف والمفهوم يخلق فجوة في العديد من المنظمات التي تتعامل مع برامج الأمن المعلوماتي، ويعرضها لكثير من المخاطر وخلق نقاط الضعف، وتسعى هذه الدراسة إلى بناء فهم واضح للقضاء على التفاوت في تعاريف

برامج أمن المعلومات واقتراح تعريف واطار عام يمكن استخدامه في المعايير الخاصة بصناعة وتطوير برامج أمن المعلومات.

اتبع الباحث أسلوب قائمة المراجعة للوصل إلى الهدف من الدراسة وتوصل إلى أن عناصر أي برنامج أمن معلومات لمنظمة ما يشتمل على ثلاثة عناصر أساسية وهي: إطار الامتثال الإداري، البيئة التقنية وأدواتها، والسياسات والمعايير المتبعة داخل المنظمة، فضلاً عن أنه وضع تعريفاً لبرنامج أمن المعلومات بأنه برنامج يهدف إلى حماية أصول المنظمة والأعمال الإلكترونية الموجودة لذلك فهو برنامج يركز على النظم المعمول بها والمخزون المعلوماتي نفسه لأن الهدف الأساسي من البرنامج هو حماية مقومات المنظمة والعمل على استدامة الأعمال نفسها لأن العمليات التي تجرى داخل المنظمة والمستفيدين منها والعاملين يمثلون مجموعة العملاء الذين يخدمهم برنامج أمن المعلومات.

هدفت دراسة الباحث Rolf H. Weber التي قام بها عام 2016[20]، إلى التعرف على التدابير التشريعية التي تقوم على حماية أمن المعلومات في بيئة الإنترنت من خلال إنترنت الأشياء ويناقش اللوائح الدولية المطبقة في هذا المجال مع المحاولة بالخروج بحلول بديلة لمعالجة القضايا الأمنية الناشئة عن المخاطر التي تهدد أمن المعلومات.

وفي هذا الصدد تناول الباحث اتفاقية بودابيست لمكافحة جرائم تقنيات المعلومات المبرمة في عام 2001 ودخلت حيز التنفيذ عام 2004، وأيضاً تناول تشريع الإتحاد الأوربي بشأن مكافحة جرائم أمن المعلومات في بيئة الإنترنت عام 2015، للوقوف على أهم النصوص القانونية والأفعال التي تعتبر بمثابة جرائم إلكترونية من وجهة نظر المشرع.

وخلصت الدراسة إلى أن سرعة التغيير والتطور التكنولوجي وتطور أساليب المهاجمين يتطلب ضرورة وجود أساليب جديدة لحماية المعلومات في بيئة الإنترنت إذ أن كل جهاز حاسب آلي متصل بالإنترنت يقع تحت تهديد هذه الجرائم مع وجود ثغرات عديدة تسهل هذه الهجمات، ويتطلب ذلك تعزيز الأمن المعلوماتي في بيئة الإنترنت بشكل عاجل وأيضاً المرونة المبتكرة بما يكفي للتصدي لهذه الهجمات، وأشاد الباحث بجهود الإتحاد الأوروبي في التدابير التشريعية وإن كانت على الأقل على الورق كما ذكر الباحث إلى أنها تلعب دوراً هاماً في الممارسة العملية لتعزيز أمن المعلومات بشكل عام.

في ضوء الدراسات العربية والأجنبية السابق ذكرها اتضحت عدة اختلافات بينها وبين الدراسة الحالية، يمكن إيجازها في النقاط التالية:

1. بدايات لتشريع يتضمن شروط تنظيم عمليات التعاقد بين المسئولين عن تقديم خدمات الإسناد الخارجي لضمان حماية أمن المعلومات.
2. معالجة التشريع الجزائري لطبيعة جرائم أمن المعلومات على الجانبين الموضوعي والإجرائي.
3. تطبيق معايير أمن المعلومات وطرق مكافحة المخاطر التي تعترض أمن المعلومات في المركز القومي للمعلومات بالسودان.
4. توافق معايير أمن المعلومات بنسب متفاوتة في مكتبة السلطان قابوس.
5. تطبيق التدابير المضادة لحماية أمن المعلومات في الشركات الصغيرة المتواجدة في بيئة الإنترنت.
6. الاهتمام بدور العامل البشري في مجال أمن المعلومات كأحد أهم مهددات أمن المعلومات الرقمية.

7. ضبط مصطلحات أمن المعلومات للتوافق مع معايير الأمن المتبع داخل منشآت أمن المعلومات.
8. تطبيق معايير أمن المعلومات في مجال أمن إنترنت الأشياء من خلال القوانين الأوروبية الخاصة بمكافحة جرائم تقنيات المعلومات.

أما دراستنا الحالية فركزت على جانب التحليل النظري لروافد أمن المعلومات الرقمية من خلال استقراء الإنتاج الفكري في أدب الموضوع.

الدراسة النظرية:

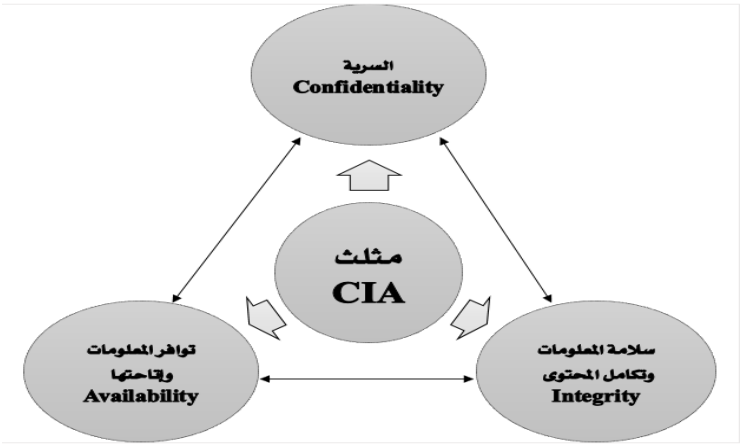
عناصر أمن المعلومات:

يعتمد أمن المعلومات على ثلاثة عناصر أساسية لابد أن يتم توافرها في المعلومات التي تستوجب الحماية، وهي السرية Confidentiality وسلامة المعلومات وتكاملها Integrity وتوافر المعلومات Availability، تُعرف باسم مثلث CIA أو CIA Triangle، ويمكن تناولها على النحو التالي[21]:

1. السرية Confidentiality: وهي القدرة على الحفاظ على سرية المعلومات عن طريق منع الدخول غير المصرح للمعلومات سواء كانت محفوظة على وسيط مادي أو يتم إرسالها عبر وسائل الاتصالات، والتأكد عدم الإفصاح عنها بالإضافة إلى عدم السماح بالاطلاع عليها إلا من خلال الأشخاص المصرح لهم بذلك.
2. سلامة المعلومات وتكامل المحتوى Integrity: التأكد من المحافظة على محتوى المعلومات وسلامته من العبث أو التعديل أو الإفساد وذلك عن طريق منع الوصول إلى هذا المحتوى عن طريق التدخل غير المشروع.

3. توافر المعلومات وإتاحتها Availability: ضمان توافر المعلومات والقدرة على تقديمها وإتاحتها في الوقت المناسب من خلال الأشخاص المصرح لهم بذلك، والتأكد من أن هؤلاء الأشخاص لن يتم منعهم من استخدام المعلومات أو الدخول إليها.

يمكن توضيح عناصر أمن المعلومات المعروفة باسم (مثلث CIA) وهي أحد أهم العناصر الأساسية لأي نظام معلوماتي وفقاً للمعايير الدولية المختصة بسياسات أمن وإدارة المعلومات، من خلال الشكل التالي:



شكل (1)

عناصر أمن المعلومات (مثلث CIA)

المخاطر التي تهدد أمن المعلومات:

بالرغم من أهمية أمن المعلومات وأهمية محتوياتها لدى مؤسسات المعلومات إلا أنها لا زالت تتعرض للكثير من المخاطر الأمنية التي تتعرض لها وتناولت العديد من الدراسات أنواع المخاطر التي تهدد أمن المعلومات وتعددت معها تصنيفات هذه المخاطر، فقد تكون ناتجة عن تهديدات طبيعية مثل الكوارث والزلازل أو من خلال

العاملين أو مستخدمين النظام أنفسهم بمؤسسات المعلومات سواء كانت بنية القصد أو من غير قصد.

فقد أشارت الدراسات أن 80% من الهجمات الناجحة على المعلومات تنشأ عن عوامل التهديد الخارجي ولكن تكون من جانب العاملين على النظام وذلك عن طريق ما يسمى بالاصطياد Phishing والخداع لأحد المسئولين عن نظام أمن المعلومات من الداخل أو عن طريق تحميل برامج ضارة مما يتيح للمهاجمين الوصول إلى النظام[22].

من خلال الاطلاع على أدبيات الموضوع التي تتناول مخاطر أمن المعلومات والتصنيفات المختلفة لها، يمكن وضع تصنيف للمخاطر التي يتعرض لها أمن المعلومات إلى ثلاثة تصنيفات مختلفة وهي: مخاطر مادية (فيزيائية) ومخاطر إلكترونية معلوماتية، ومخاطر الداخلية، وفيما يلي نتناول تصنيفات مخاطر أمن المعلومات على النحو التالي:

1 - **المخاطر المادية** Physical Threats:

هي المخاطر الناجمة عن الوصول المادي لمكونات نظام أمن المعلومات أو تلف في الموارد المتاحة لأمن المعلومات وتشمل الضرر الذي تسببه الطبيعة من كوارث طبيعية محتملة على المنشأة المعلوماتية أو السرقة أو الحريق وغيره من الحوادث الطارئة، مما يتسبب في ضرر دائم للبيانات التي تحويها هذه المنشأة، ويمكن تقسيم المخاطر المادية إلى قسمين رئيسيين:

أ- المخاطر الطبيعية Natural Threats:

تتكون الأخطار الطبيعية من الكوارث الطبيعية مثل الفيضانات والعواصف والأعاصير والزلازل الأرضية والبراكين، ويمكن التغلب على هذه الكوارث الطبيعية

والتنبؤ بها قبل حدوثها بفضل التطور التكنولوجي الحديث أو من خلال التخطيط في اختيار موقع المنشأة المعلوماتية قبل الشروع في بنائها[23].

تعد هذه الأخطار تهديدًا على شبكات المعلومات وبنيتها التحتية لأنها تقع دون سابق إنذار لذلك يجب الاحتياط دائما وعمل نسخة احتياطية Backup بشكل منتظم لمحتويات الشبكة تحفظ هذه النسخة في أماكن بعيدة عن المقر الرئيسي للشبكة الأم حتى يمكن استرجاع هذه المعلومات في حالة حدوث واحدة من تلك الكوارث الطبيعية المحتملة[24].

ب- المخاطر البيئية الطارئة Environmental threats:

تحدث هذه المخاطر من خلال اختراق مقاييس الأمن الطبيعية نتيجة سوء الاستخدام للمكونات المادية لنظام أمن المعلومات مثل أجهزة التكييف أو بسبب الغبار والأتربة وغيرها من العوامل التي تؤثر على أماكن تخزين المعلومات من الإهمال المباشر في الأماكن المخصصة لها أو غير المباشر من خلال نقاط الربط الجوهرية خارج نظام أمن المعلومات إما في إمدادات الكهرباء أو قنوات الاتصال عن بعد[25]، ويمكن أن يؤدي إلى تعطل العمل وتوقفه لفترات طويلة مما يؤثر على أمن وسلامة المعلومات.

2 - **المخاطر الداخلية** Internal Threats:

هناك العديد من المخاطر التي يكون مصدرها من داخل نظام أمن المعلومات نفسه بواسطة العامل البشري مثل العاملين أو بواسطة قصور في النظام أو اختراق للبنية التحتية له من برمجيات وأجهزة تتمثل في المكونات المادية للنظام، ويمكن تقسيم المخاطر الداخلية لأمن المعلومات إلى الأقسام الآتية:

أ- المخاطر البشرية Humans Threats:

أشارت الدراسات أن 80% من الهجمات الناجحة على المعلومات تنشأ عن عوامل التهديد الخارجي ولكن تكون من جانب العاملين على النظام وذلك عن طريق ما يسمى بالاصطياد Phishing والخداع لأحد المسئولين عن نظام أمن المعلومات من الداخل أو عن طريق تحميل برامج ضارة مما يتيح للمهاجمين الوصول إلى النظام[26].

ويقصد بالمخاطر البشرية أنها "الأخطاء التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات، أو من خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام أو في عمليات تحديد الصلاحيات الخاصة بالمستخدمين، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة المعلومات"[27].

عادةً ما يتألف الأمن البشري في أي منشأة معلوماتية من ضرورة ضمان أن يكون الأشخاص المصرح لهم بالاتصال بالنظام جديرين بالثقة ومسئولين بشكل يضمن عدم تعرضهم للضغوط التي يمكن أن تقع عليهم من خارج نظام أمن المعلومات، ويشمل نظام أمن المعلومات بالنسبة للعنصر البشري بشكل عام الفئات التالية[28]:

1. المستخدمين: هم المستفيدون من المعلومات الموجودة في المنشأة المعلوماتية.
2. مشغلي الخدمات المعلوماتية: هم الأشخاص الذين يديرون نظام أمن المعلومات.
3. المبرمجين: هم المسئولون عن برمجيات الحاسوب والأساليب التقنية المتعلقة بأمن المعلومات.
4. الزائرين: تضم هذه الفئة أولئك الأشخاص الذين لهم حق الاطلاع فقط على المعلومات دون التدخل فيها.

5. مهندسين المعلومات: هم المنوط لهم بتشغيل التطبيقات المعلوماتية وإصلاح الأخطار الواردة عليها، كما أنهم من يقومون بالمتابعة الدورية لنظام أمن المعلومات.

ب- المخاطر التقنية Technical Threats:

يغلب على هذه المخاطر الطابع الفني وتتم نتيجة تهديدات ناجمة عن القصور والثغرات الموجودة في مختلفة أنظمة أمن المعلومات، دون أي تدخل بشري أو أي تهديدات طبيعية أو بيئية ومن هذه التهديدات ما يلي:

1. تهديدات عيوب التصميم: تشمل عيوب التصميم في الأجهزة والبرامج والشبكات وأدوات الربط والتخزين، أو أي مكون آخر من المكونات المادية لأنظمة المعلومات.

2. تهديدات تشتت المعلومات: إذا كانت معلومات المنشأة مشتتة وتم تخزينها في أماكن كثير ومتفرقة يتم التعامل معها من خلال شبكات متعددة.

3. خلل في المعدات: أن تكون هذه الأعطال بسبب قدمها وعدم متابعة عمليات تجديدها وتحديثها أو بسبب الاستعمال الخاطئ.

4. أخطاء البرمجيات: قد تحتوي البرمجيات المستخدمة في أمن المعلومات على العديد من الأخطاء الأمر الذي ينعكس بالتالي على دقة المخرجات وصحة المعالجة التي يقوم بها النظام، ويتم ذلك عن طريق استخدام برامج غير أصلية أو نسخ مقلدة منها بطريقة غير شرعية.

5. أخطاء البيانات: يتعلق بأخطاء بإدخال البيانات في نظام أمن المعلومات بحيث يتم إدخال بيانات غير صحيحة مما ينعكس على دقة المعلومات المستخرجة في عمليات الاسترجاع [29].

3 - **المخاطر الإلكترونية** Electronic Threats:

تقع المخاطر الإلكترونية في الغالب من خارج النظام من قبل أشخاص ليس لهم علاقة به أو صلاحيات الدخول، وتكون هذه الاعتداءات عباره عن قرصنة المعلومات واختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات لها طالع السرية، حيث تكمن خطورة تلك المخاطر في عدم معرفة من قام بالاختراق وماهي حدود قدرته في التخريب بالإضافة إلى عدم معرفة الهدف من وراء هذه الاختراقات[30].

منذ وقت قريب كانت المخاطر الإلكترونية تتعلق بتقنيات الحاسب الآلي ونظم المعلومات وما يتعلق بالمعالجة الآلية للمعلومات، حيث كانت تدور هذه المخاطر حول التلاعب في البيانات المدخلة للحاسب الآلي والاعتداءات التي تقع على المخرجات وسرقة البيانات عن طريق الاختراق، ويمكن تصنيف جرائم الحاسب الآلي إلى ثلاثة أنواع[31]:

1. الجريمة المحوسبة: وتكون الجريمة عبارة عن سوء استخدام أجهزة الحاسب الآلي بشكل غير قانوني، يؤدي إلى ارتكاب جريمة يعاقب عليها قوانين جرائم الحاسب الآلي.
2. سوء الاستخدام لجهاز الحاسب الآلي: يكون سوء الاستخدام بشكل مقصود للتسبب في التخريب للأجهزة والتلاعب بالمعلومات.
3. الجرائم المتعلقة بالحاسب الآلي: التي يكون فيها الحاسب الآلي نفسه أداة لتنفيذ الجريمة.

ويمكن أن تتم الجرائم الخاصة بالحاسب الآلي من العاملين داخل المنشأة المعلوماتية الذين لديهم صلاحيات التعامل مع النظام، حيث أشارت الدراسات إلى أن الخسائر الناتجة عن جرائم الحاسب الآلي ومنها دراسة أجرتها دائرة المحاسبة العامة

وشركة أوركاند Orkand للاستشارات، أن حجم الخسائر المتعلقة بجرائم الحاسب الآلي تقدر بحدود 1.5 مليون دولار لشركات المصارف المحسوبة في الولايات المتحدة الأمريكية، ومن ناحية أخرى يقدر المركز الوطني لبيانات جرائم الحاسب الآلي في لوس أنجلوس بنحو 70% من جرائم الكمبيوتر تزداد بصورة واضحة[32]، مما يجعلها تشكل تحدياً خطيراً يواجه الإدارات العليا بشكل عام وإدارة نظم المعلومات بشكل خاص.

جدير بالذكر أن ظهور الجريمة الإلكترونية أو السيبرانية كان نتيجة التطور التكنولوجي في نظام الاتصالات وخدمات الإنترنت، ويمكننا تصنيف الجرائم التي تتم عن طريق استخدام تكنولوجيا المعلومات من خلال الحاسب الآلي إلى الأقسام الآتية[33]:

- جرائم نشر المعلومات السرية.
- جرائم التزوير الإلكترونية.
- جرائم ترويج الإشاعات.
- جرائم تقنية المعلومات.

أشكال المخاطر التي تهدد أمن المعلومات.

تعددت أشكال ونماذج المخاطر التي تهدد أمن المعلومات فمنها ما يتعلق بالمخاطر الناتجة عن الجرائم الخاصة بالاعتداء على محتوى الحاسب الآلي سواء في مكوناته المادية أو المكونات المعنوية وقواعد البيانات أو المعلومات التي تكون ضمن محتويات الحاسب الآلي، أو الجرائم المتعلقة بمحتويات الشبكة العالمية التي تستخدم من خلال الحاسب الآلي وتكون وسيلة للربط بين الحواسب الآلية وما ينتج عن ذلك من الجرائم السيبرانية، وفيما يلي نتناول بإيجاز قدر الإمكان لأهم نماذج هذه المخاطر في ضوء تصنيفات المخاطر التي تهدد أمن المعلومات السالفة الذكر وذلك على النحو التالي:

1 - **هجوم تعطيل الخدمة** Denial Of Services (DOS):

يتم هجوم تعطيل الخدمة عن طريق إرسال عدد هائل من طلبات الاتصال أو أوامر بروتوكولات الشبكات مثل أمر Ping إلى الجهاز الضحية من أجل إغراقه في معالجة هذه الطلبات مما يحمل الحاسب الآلي أكثر من طاقته حتى يتوقف عن الاستجابة، ومن ثم عدم قدرته على القيام بمهامه، وقد تصل درجة الإغراق Flooding إلى تعطيل الهدف نهائيا والخروج من الخدمة.

يستهدف هجوم تعطيل الخدمة عبر خدمات الإنترنت ثلاثة أنواع مختلفة وهم: المستخدم وجهاز الحاسب الآلي المضيف للخدمة بالإضافة إلى شبكة الاتصال، حيث يبدأ هجوم تعطيل الخدمة باستخدام أدوات ترسل عبر الإنترنت مثل تعرف باسم Trin00, Tribe Flood Network, Stacheldraht وهي أدوات خاصة بإغراق الحاسب الآلي بالأوامر المتتالية حتى يقف عن الاستجابة ومن ثم يمكن استغلال الثغرات في وقت توقف الحاسب الآلي للوصول غير المصرح به للبيانات واستخدام بعض الأساليب لإتلاف البيانات وتعطيل الخدمة ومنع المستخدمين الشرعيين من الوصول إليها[34].

2 - **الهندسة الاجتماعية** Social Engineering:

أشار ساجار رالكار Sagar Rahalkar إلى أن الهندسة الاجتماعية هي الفن الخادع في التواصل مع الناس من أجل الحصول على معلومات هامه تأخذ الشكل السري، ومعظم الناس لا يعلمون مدى قيمة المعلومات التي يمتلكونها، فنجد المهاجمين يقومون باستخدام العديد من الحيل المختلفة لإقناع الضحية بتقديم هذه المعلومات عن طريق الادعاء بأنه مسئول مُعترف به كما هو الحال في سرقات أرقام بطاقات الائتمان فيدعي هنا المهاجم بأنه مسئول بنك من البنوك الشهيرة ثم يسأل الضحية عن رقم الائتمان الخاص به أو رقم التعريف الشخصي الخاص به[35].

ومن خلال هجمات الهندسة الاجتماعية يستخدم المهاجمون مجموعة من التكتيكات المتنوعة لإنجاز أهدافهم، ويمكن أن تكون حيلة بسيطة مثل اكتساب ثقة الضحية عبر الهاتف للحصول على معلومات سرية لإعداد الطُعم لشخص ما للوصول إلى موقع الويب المُخترق من خلال ما يسمى بالاصطياد الإلكتروني[36].

3 - **الاصطياد الإلكتروني** Phishing:

يعتبر الأسلوب النموذجي للجمع بين جرائم خداع الهندسة الاجتماعية وتكنولوجيا الشبكات، الذي يتم عن طريق عمل موقع إلكتروني مزيف لموقع إلكتروني قائم بالفعل بهدف خداع المستخدمين، ويكون ذلك عادةً من خلال الرسائل غير المرغوب فيها عن طريق البريد الإلكتروني ورسائل الهاتف المحمول بالإضافة إلى الإعلانات الكاذبة التي تظهر بشكل مفاجئ خلال تصفح محتويات المواقع الإلكترونية ومن خلالها سرقة حسابات البريد الإلكتروني أو أرقام الحسابات البنكية وغيرها من المعلومات الهامة[37].

ترجع تسميته بهذا الاسم إلى عام 1996 حيث كان قبلها يطلق عليه مصطلح الصيد قبل أن يتغير إلى الاصطياد الإلكتروني، كما أن أول حادثة تمت باستخدامه كان ضحيتها موقع أمريكا أون لاين America Online (AOL) في عام 1990، لأنه من أجل فتح حساب للحصول على خدمات الموقع يجب على المستخدم أن يكتب تفاصيل بطاقته الائتمانية كاملة ثم قام المهاجمون بعمل موقع مزيف مماثل للموقع الأصلي، من خلاله تمت سرقة ملايين البيانات البنكية الخاصة بالمشتركين في موقع أمريكا أون لاين[38].

يتم خداع المستخدمين عن طريق الرسائل المزيفة السالف ذكرها التي تحتوي على روابط لمواقع إلكترونية مزيفه تشابه الموقع الإلكتروني الأصلي، وبالتالي يقوم المستخدم بالدخول على تلك المواقع وملئ البيانات التي تعوّد على كتابتها عند

تصفحه للموقع الأصلي مثل معلومات حسابه البنكي أو معلومات خاصة بمواقع أخرى هامه وبذلك يقع المستخدم ضحية لجرائم الاصطياد الإلكتروني، لإن الموقع المزيف يكون متماثل من حيث الواجهة الرئيسية للموقع الأصلي مثل ألوان التصميم والأشكال ويمكن أن يختلف الموقع المزيف عن الأصلي بفرق بسيط كحرف زائد أو ناقص عن عنوان الموقع الأصلي ونتيجة لهذا التشابه فلا يستطيع المستخدم العادي أن يفرق بين الموقع الأصلي والمزيف[39].

4 - **البرمجيات الضارة** Malware:

تعد البرمجيات الضارة من أعظم الاعتداءات التي تتعرض لها أنظمة المعلومات التي تصيب أجهزة الحاسب الآلي والهاتف المحمول في حالة اتصاله بخدمة الإنترنت، وتشير البرمجيات الضارة على وجه العموم إلى برنامج أو كود يمكن زرعه سراً في جهاز الضحية بدون إذن منه بغرض إحداث الضرر فيه أو تعطيله أو القيام بأي إجراء غير مشروع على المعلومات التي يحتويها جهاز الضحية[40].

أما بالنسبة لأنواع البرامج الضارة فقد قسمها أستاذ أمن المعلومات مارتينيز توريس Martinez Torres إلى ثلاث فئات رئيسية من حيث الاعتماد على كيفية انتشارها عبر شبكات الإنترنت وهي الفيروسات وأحصنة طروادة والديدان[41]، وهي على النحو التالي:

أ- الفيروسات Viruses:

بدأ ظهور الفيروسات في السبعينات من القرن الميلادي الماضي، وكانت درجة خطورتها بسيطة في البداية ليست على مستوى الخطورة الموجودة في الوقت الحاضر، ثم أصبحت أكثر خطراً وانتشاراً عن السابق نظراً لتزايد استخدام الحاسب الآلي وانتشار خدمات الإنترنت، لذلك تعد أكبر فئات البرامج الضارة من حيث تعدد أشكالها وأنواعها.

وأشار فيرناندو جورجيل Fernando Georgel إلى أن الفيروسات عبارة عن البرامج التي يمكن أن تصيب برامج أخرى عن طريق تغييرها أو بنسخها مره أخرى بداخل برامج الحاسب، وتمر دورة حياة الفيروسات بعدة مراحل حتى تتمكن من إلحاق الضرر بجهاز الحاسب الآلي، وهم أربع مراحل نتناولهم على النحو التالي[42]:

1. مرحلة الخمول: عندما يكون الفيروس خاملاً في انتظار تنشيطه من قبل المستخدم.
2. مرحلة الانتشار: تحدث عندما يقوم الفيروس بإنشاء نسخة من نفسه وإدراجها في برنامج معين من البرامج المحفوظة على جهاز الحاسب الآلي.
3. مرحلة التفجير: يقوم فيها الفيروس بالتحرك في تنفيذ وظائفه المطلوبة منه.
4. مرحلة التنفيذ: يقوم الفيروس بالبدء في التصرف على النحو المطلوب منه في تدمير البرامج أو تسريب المعلومات وإتلافها.

ب- أحصنة طروادة Trojans Horses:

تعد أحصنة طروادة من البرمجيات الضارة التي تظهر في شكل برامج مشروعة ولكنها تخفي في داخلها برامج ضارة حتى يقوم الضحية بتثبيتها على جهازه أو تشغيله ثم يتمكن المخترق من الوصول عن طريقها إلى جهاز الضحية، لذلك أطلق على هذه البرمجيات إسم أحصنة طروادة نسبة إلى القصة اليونانية المشهورة التي قام الإغريق بالتسلل داخل حصان خشبي ضخم مخبئ بداخلة الجنود حتى يتثنى لهم الدخول إلى أراضي العدو كتمويه لاكتساب الحرب[43].

وفي حالة ما إذا قام المستخدم للجهاز الضحية بتشغيل البرامج التي تحتوي على أحصنة طروادة يتم حينها تنشيط البرامج الضارة المخبأة بداخلها وتعمل على ممارسة عملها الذي صممت خصيصًا للقيام به وغالبًا ما يكون الغرض منها هو

التجسس، حيث تسمح هذه البرمجيات بالتحكم في الجهاز الضحية أثناء الاتصال بخدمة الإنترنت وتصفح محتوياته فضلاً عن تنفيذ الأوامر المتعلقة به[44].

ج- الديدان Worms:

على عكس الفيروسات التي تتطلب من الضحية اتخاذ بعض الخطوات للتعرض للفيروسات مثل نسخه من مصدر آخر مصاب أو تنشيطه بالخطأ، فإن الديدان لها القدرة على الانتشار بشكل سريع عبر الإنترنت ويكون الهدف منها عادة نفس الأهداف الخاصة بالفئتين السابقتين وهو إحداث الضرر بأنظمة الكمبيوتر لتدمير المعلومات التي يحتويها، أو لجمع المعلومات الشخصية بدون علم صاحب جهاز الحاسب الآلي[45]، وعادة ما تنتشر ذاتيًا عبر شبكة الإنترنت من خلال نقاط الضعف التي تتسبب في وجود الثغرات الأمنية الموجودة في نظام أمن المعلومات[46].

5 - **برمجيات التجسس** Spyware:

تعتبر برامج التجسس نوع آخر من البرمجيات الخبيثة التي تتوافر فيها الأغراض غير الشرعية فهي تعمل على مراقبة كل ما يكتبه الضحية حتى أنه تسجل النقرات على لوحة المفاتيح وترسلها إلى المُخترق وتقوم أيضا على أعمال خبيثة أخرى[47].

البرامج الضارة التي تقوم بتنفيذ مهامها بشكل مستقل عن طريق الاتصال بالشبكات الاجتماعية أو موقع ما على شبكة الإنترنت، وتقوم هذه البرامج بجمع معلومات حول ما يقوم به المستخدم من أنشطه سواء عبر الإنترنت أو في وضع عدم الاتصال بالإنترنت على الجهاز الخاص بالضحية وإرسال هذه المعلومات للمَخترق فور اتصال الحاسب الآلي بالإنترنت[48]، ولبرامج التجسس أنواع عديده نذكر منها ما يلي:

- برامج التجسس البسيط ومتابعة نشاط المستخدم.

- برامج تسجيل نقرات لوحة المفاتيح Keyloggers.
- برامج الإعلانات Adware.
- النوافذ الفقاعية أو المنبثقة Popup.

6 - البريد الإلكتروني غير المرغوب Spamming **:**

ويتم في هذا النوع من الهجمات استخدام البريد الإلكتروني كوسيلة لإغراقه بالرسائل الدعائية لمنتجات معينة مما يستهلك موارد الحاسب الآلي ويتطلب ذلك كثيراً من الوقت والمال مما يؤدي إلى خنق الشبكة والعمل على إبطائها في نقل البيانات وسرعة استجابة خدمة الإنترنت نفسها.

يرجع السبب لاختيار البريد الإلكتروني ليكون البيئة التي يتم من خلالها شن مثل هذا النوع من الهجمات إلى أن العلاقات الاجتماعية القائمة بين المستخدمين وخاصة في مواقع التواصل الاجتماعي تكون قائمة على الثقة الوهمية، مما يعني أنه من السهل إقناع المستخدم المستهدف بقراءة محتوى البيانات غير المرغوب فيها ويرجع ذلك إلى الإيهام بأنها رسائل آمنه ونتيجة لذلك يمكن أن تطور هذه الهجمات إلى جرائم الاصطياد الإلكتروني Phishing[49].

جدير بالذكر أن تلك الأنواع التي تم تناولها تعتبر أهم نماذج وأشكال المخاطر التي تتعرض لها أمن المعلومات في بيئة الإنترنت، بالإضافة إلى العديد من الأنواع الأخرى مثل مخاطر هجمات الانتحال Spoofing Attacks وهجمات اعتراض البيانات Sniffer Attacks وغيرها من المخاطر التي لا يتسع المجال لذكرها.

التدابير الأمنية لحماية أمن المعلومات:

من خلال تناول مخاطر أمن المعلومات السالف ذكرها كانت هناك حاجة ماسة لتوفير التدابير الأمنية الكافية لحماية أمن المعلومات من هذه المخاطر بالإضافة

إلى إيجاد تقنيات مبتكرة تضمن شرعيتها وتأمينها من تلك المخاطر، ويمكن تقسيم التدابير الأمنية اللازمة لحماية أمن المعلومات إلى أربعة أقسام رئيسية وهي: التدابير التنظيمية، المادية، التقنية، بالإضافة إلى التدابير التشريعية لضمان توفير حماية أمن المعلومات، وفيما يلي تناول هذه التدابير على النحو التالي:

أولا: التدابير التنظيمية Organizational Measures:

تتعلق التدابير التنظيمية بالأنشطة الإدارية داخل مؤسسات أمن المعلومات، حيث تهدف هذه التدابير لبناء بيئة آمنة للمعلومات والحفاظ عليها من خلال مجموعة من الإجراءات الإدارية الأمنية المضادة ويتم اختيارها للتطبيق بشكل فعال داخل مؤسسات أمن المعلومات[50]، ويمكن تقسيم التدابير التنظيمية إلى قسمين هما: تدابير إدارية وأخرى شخصية خاصة بالعاملين في مؤسسات المعلومات، نتناولهما كما يلي:

أ- التدابير الإدارية:

يُراد بالتدابير الإدارية سيطرة جهة الإدارة على إدارة نظم أمن المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية أو الأجنبية عن المنشأة، فضلا عما يتعلق بمسائل الإشراف والمتابعة على أنشطة المؤسسة في الرقابة على الاشتراكات الخارجية للمنشأة مع المؤسسات الأخرى ومسائل التحقيق في المخاطر التي تتعرض لها المنشأة[51].

ويمكن توفير التدابير الإدارية للازمة لحماية أمن المعلومات من خلال مجموعة من التعليمات والإرشادات مثل سياسات أمن المعلومات واستراتيجيات إدارة أمن المعلومات، حيث يتم اعتماد هذه السياسات لتحديد طرق استخدام المعلومات ومصادرها بشكل آمن وعمل الوثائق اللازمة لمراقبة التعامل مع المعلومات، كما يتم المراقبة على السلوكيات الغير مألوفة سواءً من العاملين داخل المنشأة أو

خارجها، ويجب توثيق هذه السياسات في وثائق مكتوبة وتعميمها على العاملين بالمنشأة لزيادة الوعي والاهتمام بأمن المعلومات[52].

ب- التدابير الشخصية:

تتعلق التدابير الشخصية بحماية المعلومات على مستوى الأفراد العاملين على نظام أمن المعلومات حيث يشكل الأفراد العاملون على النظام أحد أهم التهديدات القوية التي يمكن أن تؤثر على أمن وسلامة المعلومات، فقد يرتكب الفرد خطأ عند استخدامه لنظام أو أثناء إعداد وتجهيز البرامج الخاصة بالمنشأة مما يقلل من فعاليتها كما يجب عدم إغفال أن أعظم التهديدات تأتي قد تأتي من العاملين على النظام[53].

ترتبط حماية العاملين في النظام بوسائل التعريف الخاصة بهم والتأهيل والتدريب للمتعاملين مع وسائل الأمن إلى جانب الوعي بمسائل الأمن ومخاطر الاعتداء على أمن المعلومات، لذا فإن أهم الإجراءات التي يمكن أن تساعد المنشآت المعلوماتية على اتخاذ التدابير اللازمة لحماية أمن المعلومات من التهديدات التي قد تحدث من العاملين لديها ما يلي[54]:

1. تحديد كلمات مرور للعاملين على أن يراعى تحديد صلاحيات كل موظف بما يتناسب مع طبيعة عمله، وتكون قاصرة على نطاق عمله بالمنشأة فقط وليست صلاحيات دون حدود.
2. اختيار العاملين بعناية تامة مع ضرورة التأكد من أمانتهم وإخلاصهم ويظهر ذلك من خلال قيام الإدارة بمراقبة سلوكياتهم عن بُعد للتأكد من ذلك.
3. تدريب العاملين بشكل جيد تجنباً للعديد من المشكلات التي قد تواجهها الشبكة.
4. التأكد من إزالة بيانات العاملين المنتهية مدة خدمتهم في المنشأة من قائمة مستخدمي النظام.

ثانيا: التدابير المادية Physical Measures:

يُطلق مصطلح التدابير المادية على كافة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها مثل الأقفال والحواجز والغرف المحصنة وغيرها من الوسائل التي تقوم على حماية الأجهزة الحساسة من العبث أو التخريب، ولتحقيق المستوى المطلوب من الحماية المادية لأمن المعلومات لابد من مراعاة عدة عوامل، منها ما يلي[55]:

1. تخصيص غرف مغلقة لحماية أجهزة خادم الشبكة المركزية للمنشأة أي بعيداً عن غرف العاملين أو المستفيدين حتى لا يكون متاحاً للجميع.
2. استخدام الكابلات المغلفة وذلك لتقليل الإشعاع الثانوي المنبثق من خلالها، مع إمكانية إضافة أكثر من غلاف عليها لمنع هذا الإشعاع.
3. توفير وسائل مراقبة لموقع المنشأة من الداخل والخارج مثل الدوائر التلفزيونية المغلقة.
4. تأمين الأبواب والمنافذ وذلك باستخدام أجهزة الإنذار الآلية لتقوم بتشغيل أجراس التنبيه في حالة الدخول في غير ساعات العمل الرسمية.
5. تركيب الكابلات الخاصة بالشبكة عبر تمديدات عبر الجدران أو فوق الأسقف حتى لا تكون معرضه لوصول غير المختصين.

فضلاً عن أن هناك طرق أخرى وأدوات تساعد المنشأة على تحقيق الأمن المادية وحمايتها من التهديدات وهذه الطرق تتداخل مع التدابير التقنية لأمن المعلومات ولكن سنتناول فقط ما يتعلق بالأمن المادي لأمن المعلومات، من هذه التدابير نذكر ما يلي:

1. التحكم في الوصول Access Control:

يعتبر التحكم في الوصول من التدابير المادية الهامة والحساسة في أمن المعلومات، فجميع أنظمة أمن المعلومات تحتاج أن تعمل في بيئة آمنة بعيدة عن أيدي غير المتخصصين حتى لا يؤثر ذلك على كفاءتها مثل العبث والتخريب أو الأعطال بسبب العوامل الطبيعية المختلفة مثل الحرائق والزلازل أو انقطاع التيار الكهربائي.

تبين أن التحكم بالوصول بالنسبة للتدابير المادية ينقسم إلى شقين: الشق المادي ويتعلق بالتدابير المادية مثل الحواجز الفيزيائية المادية لحماية الموارد المادية والمنشآت، والشق التقني الخاص بتصاريح الدخول الخاصة بالعاملين في المنشأة مثل كلمات السر وبطاقات الدخول الممغنطة بالإضافة إلى القياسات الحيوية Biometrics للتحكم بالوصول لخدمات المنشأة، فيما يلي سنتناول الشق المادي:

أ- الحواجز الفيزيائية Physical Barriers:

تتعلق الحواجز الفيزيائية بالوسائل التي تساهم في منع الوصول إلى الموارد الحيوية في منشأة المعلومات من أجهزة وشبكات وغيرها ولتطبيق ذلك لابد من توافر التدابير الآتية[56]:

1. وضع ما يسمى بحواجز محيط المنشأة Perimeter الذي يتعلق بحماية محيط المنشأة الخارجي مثل الجدران الخارجية وصافرات الإنذار.
2. وضع حواجز أمام مدخل مراكز الأجهزة وإقفالها منعًا لتعرضها لبرامج التجسس وغيرها.
3. التحكم من خارج المنشأة عن طريق البوابات المغلقة وسجلات الدخول وأجهزة المراقبة.

ب- الكاميرات ونظم المراقبة:

تساعد الكاميرات ونظم تحقيق الهوية للموظفين والمترددين على المنشأة من حفظ الأمن المادي لأمن المعلومات وذلك من خلال مراقبة الدخول والخروج من وإلى المنشأة وتحديد هوية المصرح لهم بالتواجد في المكان الذي يوجد فيه الحاسب الآلي، وتساعد كاميرات المراقبة على رصد أي نشاط من جانب أفراد غير مصرح لهم بالتواجد في أمكان وجود الأجهزة الحساسة، وأيضا تعد دليلاً في حالة ارتكاب أي تهديدات على أمن المعلومات[57].

2. نظم الإنذار المبكر:

تستخدم كنوع من التدابير اللازمة لحفظ أمن محيط المنشأة بالإضافة إلى حماية الموارد التقنية والمادية الموجودة بها، وتستخدم هذه النظم العديد من الأجهزة الحساسة الخاصة بالإنذار المبكر Sensors لرصد أعمال السرقة والحريق والعديد من الكوارث الطبيعية مثل الزلازل والبراكين وغيرها وتستخدم أجهزة أخرى لرصد المواد المشعة والسامة للحفاظ على الأمن المادي للأجهزة[58].

ثالثا: التدابير التقنية Technical Measures:

هناك العديد من التدابير التقنية التي تهدف إلى حماية أمن المعلومات من المخاطر الداخلية والخارجية والعمل على الحد منها، سنتناول أهم هذه الوسائل على النحو التالي:

1- برامج مكافحة للفيروسات Antivirus Software:

هي البرمجيات التي تستخدم لاكتشاف وإزالة كافة أنواع البرمجيات الضارة والخبيثة والعمل على محوها تماماً من النظام لما لهذه البرمجيات من تهديدات قد تؤثر على أمن المعلومات التي تضمها المنشأة[59].

وعملت العديد من شركات الحماية على تطوير برامج مضادة للأنواع الحديثة من الفيروسات التي تنتشر في البيئة الإلكترونية ومن أمثلتها MacAfee, Kaspersky, Norton, Avira, Avast وغيرها من الشركات، ولكي تكون برامج مكافحة الفيروسات قادرة على القيام بعملها بشكل متكافئ وفعّال لابد من تمتعها بعدد من السمات الواجب توافرها، نذكر منها ما يلي[60]:

1. أن يكون مدمجاً بداخلها جدار ناري Firewall للتصدي لأي محاولات لاختراق بنية نظام أمن المعلومات، ويقوم بالتحديث التلقائي لنفسه للتعرف على الأنواع الحديثة من البرمجيات الضارة.
2. أن تتمكن هذه البرامج من فحص البريد الإلكتروني للمستخدمين بشكل مستمر والعمل على كشف أي تهديدات يمكن أن تحدث مثل جرائم الانتحال وغيرها.
3. أن يكون ذو استهلاك قليل لموارد الحاسب الآلي الموجود فيه حتى لا يتسبب في بطء الحاسب الآلي وتوقفه عن العمل في حالة القيام بعمليات البحث عن الفيروسات.

2- برامج الجدران النارية Firewalls:

تعمل هذه الفئة من البرامج على تأمين المنافذ Ports الموجودة في الحاسب الآلي التي من خلالها تتمكن التطبيقات من على الحصول على خدمات الإنترنت، وفي كثير من الأحيان لا يعلم المستخدم بالمنافذ المفتوحة على النظام مما يسمح بنسيان تأمين هذه المنافذ وحمايتها، فتعمل برامج الجدران النارية كمصفاة تمنع وصول البرمجيات الضارة إلى الأجهزة عن طريق هذه المنافذ المفتوحة[61].

وتقوم الجدران النارية على حماية أجهزة الحاسب الآلي أو شبكة تربط العديد من الأجهزة من الاختراقات من طرف جهة ثالثة، حيث يقوم بتصفية حزم البيانات المتبادلة مع الشبكة، وتنقسم الجدران النارية إلى نوعان وهما:

- الجدران البرمجية: يستخدم هذا النوع على الحاسبات الآلية المستقلة أو المرتبطة بشبكات الإنترنت أو على الخوادم ومن أبرز أنواع هذه الجدران Norton, Kaspersky.
- الجدران المادية: وتسمى أحيانا بالعلب السوداء حيث تستخدم على الأجهزة الخادمة التي تقوم على تزويد الأجهزة الأخرى بخدمات الإنترنت وهي أكثر أمنا من الجدران النارية البرمجية ومن أمثلتها SOHO WatchGuard[62].

3- التشفير Encryption:

يعتبر التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فلا يمكن معرفة فحوى المعلومات المرسلة من قِبل أي شخص آخر غير الشخص المرسلة إليه تلك المعلومات ويكون مالكاً لمفتاح فك تشفيرها مع ملاحظة أنه في حالة وصول تلك المعلومات إلى أشخاص آخرين فإنهم لا يستطيعون الاستفادة منها أو حتى فهم معناها[63]، وينقسم إلى نوعين أساسين وهما كالتالي[64]:

أ- التشفير المتماثل Symmetric Encryption:

يسمى أحياناً بالتشفير المتناظر أو باسم تكنولوجيا تشفير المفتاح الخاص، ويستخدم في هذا النوع من التشفير مفتاح واحد للتشفير وفك الشفرة وبذلك فإنه يكون معلوماً بين مرسل المعلومات والمستفيد منها، ويرسل مفتاح فك التشفير بوسيلة أخرى بعيداً عن المعلومات المرسلة، ويوضح الشكل التالي طريقة عمل التشفير المتماثل:

شكل (2)

التشفير المتماثل Symmetric Encryption[65]

ب- **التشفير غير المتماثل** Asymmetric Cryptography:

يستخدم في هذا النوع مفتاحان لكل مستخدم للمعلومات يكون إحداهما معروفاً من قِبل المستخدمين الآخرين في حالة الرغبة في إرسال معلومات مشفرة إلى شخص آخر على علم بالمفتاح الأول، ولفك التشفير يستخدم مفتاح خاص لا يعرفه سوى مستقبل المعلومات نفسه، ويمكن توضيح طريقة عمل التشفير غير المتماثل من خلال الشكل التالي.

شكل (3)

التشفير غير المتماثل Asymmetric Cryptography[66]

أتى التشفير الغير متماثل لإصلاح عيوب ومشاكل النوع السابق من التشفير حيث كانت تواجه مشكلة التوزيع غير الآمن للمفاتيح المستخدمة في التشفير المتماثل، فيتم استخدام مفتاحين إثنين تربط بينهما علاقة ما لزيادة الأمان والتعقيد في محاولة فك تشفير المعلومات المشفرة باستخدام التشفير الغير متماثل.

4- أنظمة كشف الاختراق Intrusion Prevention System:

تعمل هذه الأنظمة على منع التسلل ورصد المحاولات المتكررة للاستغلال حتى إذا لم يتم إصلاح نقاط الضعف التي يجري استغلالها، ويمكن لهذه الأنظمة أن تقدم إشعارات فورية لهذه المحاولات وأن تمنع هجمات مستهدفة معينة وقت حدوثها. حيث إن نقاط الضعف في نظم أمن المعلومات تكون المصدر الأول لعمليات التسلل، وعادةً تكون هذه النقاط التي تمثل ثغرات داخل النظام موجودة نتيجة لسوء الاستخدام من قِبل العاملين على النظام[67].

تختلف أنظمة كشف الاختراق عن برامج الجدران النارية في أنها تقوم في فحص حركة المرور للمعلومات من وإلى المستخدمين للكشف عن الهجمات المتوقعة عكس برامج الجدران النارية التي تفرض قواعد صارمة على حركة المرور وإغلاق المنافذ التي يمكن استغلالها في عمليات الاختراق فيقوم بفحص المعلومات المتداولة واتخاذ قرار السماح بمرور هذه المعلومات أو منعها في حالة الشك في أنها محاولات لاختراق النظام، لذلك فإن برامج كشف الاختراق أقل نضجاً من الجدران النارية ولكنها أكثر تعقيداً في طريقة العمل[68].

5- التحكم بالوصول Access Control:

سبق وأن تناولنا التحكم بالوصول في التدابير المادية ولكن من الناحية المادية الخاصة بحماية أمن موارد المنشأة وما يتعلق بأمن المحيط من حيث المنشآت المادية والأجهزة الإلكترونية التي تحتويها هذه المنشأة، وهنا نتناول تدابير التحكم في

الوصول من الجانب التقني وما يتعلق بالوسائل التكنولوجية الحديثة لفرض الحماية على أمن المعلومات، وتتخذ المنشأة العديد من الوسائل التقنية لتحقيق الخطوات السابق ذكرها مثل بطاقات الهوية وكلمات السر والبطاقات الذكية ووسائل التعريف البيولوجية أو ما يسمى بالقياسات الحيوية، وسنتناول أهم هذه الوسائل في النقاط التالية:

أ- كلمات السر Passwords:

يمكن لكلمات السر أن تكون عبارة عن كلمة أو جملة تستخدم للدخول إلى النظام والمصادقة عند الدخول مثل سؤال: ماذا تعرف؟[69]، أو أي طريقة لكتابة كلمات السر ولكن بشرط أن تكون معقدة وغير قابلة للتخمين، ويجب اتخاذ عدد من الخطوات عند إعداد كلمات المرور نذكر منها ما يلي[70]:

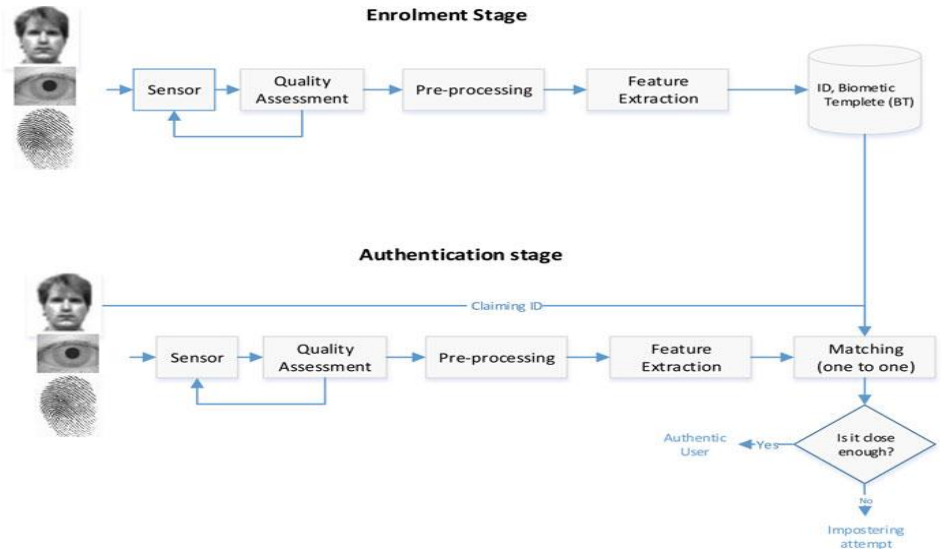
1. لا تضمن بيانات شخصية مثل تاريخ الميلاد وغيره.
2. أن تكون صعبة وغير قابلة للتخمين وتكون خليطاً بين الحروف والرموز والأرقام.
3. عدم إطلاع الغير عليها بأي شكل، مع ضرورة أن يتم تغييرها بشكل دوري.

ب- البطاقات الذكية Smart Cards:

تستخدم البطاقات الذكية كتقنية من تقنيات التحكم بالوصول حيث يختزن فيها معلومات عن المستخدم مثل أسمه وبياناته الشخصية وكلمة المرور الخاصة به على شريط ممغنط يستخدم عند رغبة الشخص في الدخول إلى نظام المعلومات واستخدام مواردها وذلك بتمرير البطاقة من خلال ماسح رقمي يعمل على ترجمة البيانات المختزنة عليها ومقارنتها ببيانات الشخص على النظام، ويسمح له بالمرور عند تطابق هذه البيانات بين البطاقة والنظام[71].

ج- تقنيات القياسات الحيوية Biometrics:

تهدف تقنيات القياسات الحيوية في التدابير المتعلقة بالتحكم بالوصول إلى تحديد هوية المستخدم والتحقق منها استناداً على بعض الخصائص البيولوجية التي لا يمكن تكرارها بين شخص وآخر مثل الوجه والأذن وقزحية العين وبصمات الأصابع، والحمض النووي أو الخصائص السلوكية للإنسان مثل الصوت وطريقة المشي والتوقيع[72]، ويوضح الشكل التالي عملية حفظ عينات من الخصائص البيولوجية للمستخدم والمصادقة عليها من قِبل النظام للسماح له بالدخول عند الحاجة:



شكل (4)

طريقة عمل نظم القياسات الحيوية Biometric systems[73]

يوضح هذا الشكل استخدام طريقتين للتحقق من هوية المستخدم: الأولى تسمى طريقة التسجيل Enrolment Stage يتم فيها أخذ عينة من أحد الخصائص

البيولوجية مثل تفاصيل الوجه وقزحية العين وبصمات أحد الأصابع عن طريق مسح بيولوجي لهذه الخصائص وتخزينها في ملف خاص بالمستخدم مدمج بالنظام.

وعند محاولة الشخص الدخول إلى النظام تتم الطريقة الثانية وهي مرحلة المصادقة والتحقق من الهوية Authentication Stage حيث تتم مقارنة الخصائص البيولوجية لهذا الشخص كما في الشكل الموضح وعند المطابقة يُسمح له بالدخول إلى شبكة النظام.

6- التخزين الاحتياطي Backup:

يقصد بالتخزين الاحتياطي مجموعة الإجراءات والمعلومات والبرامج التي يجب توفيرها في أماكن مخصصة خارج المقر الرئيسي للمنشأة وذلك للرجوع إليها في حالة حدوث ما يمنع استخدام النظام الأساسي المعمول به داخل المنشأة، سواء كان ذلك بسبب عرضي أو متعمد ونظراً لارتفاع تكاليف تأسيس نظام تخزين متكامل هناك بعض الخيارات التي يمكن للمنشأة أن تتخذها في عمل نظام تخزين احتياطي لمحتوياتها منها ما يلي[74]:

أ- نظام احتياطي متكامل:

يكون هذا النظام ذات تكلفة عالية لما يتطلبه من إجراءات وتجهيزات كبيرة تماثل النظام الأساسي المستخدم في المنشأة من حيث الأجهزة والإيدي العاملة والمتخصصين.

ب- مركز فرعي لنظام التخزين:

في هذا الخيار يكون للمنشأة أحد الفروع الذي يتم اعتباره مركزاً احتياطياً للنظام الأساسي بحيث يزود ببعض أجهزة التخزين ويتم ربطه بالشبكة الأم واستخدامه كبديل في حالة حدوث أي أخطار تعترض النظام الأساسي.

ج- الاتفاق المتبادل:

يتم الاتفاق بين منشأتين بحيث يكون لديهما تماثل في نفس الأنظمة المستخدمة بحيث يتم اعتبار أحدهما مركز تخزين احتياطي للأخر في حالة تعرض أحدهما لأي حدث طارئ والعكس مع المنشأة الأخرى، ويعد هذا الخيار أقلهم تكلفة وتوفيراً للجهد المبزول في إنشاء مركز تخزين احتياطي.

7- التوقيع الرقمي Digital Signature:

يعتبر التوقيع الرقمي تأشيرة على الوثيقة باستخدام ما يسمى بالمفتاح الخاص الذي يكون لدى المرسل للمعلومات فقط فهو ليس التوقيع التقليدي، حيث تحول المعلومات إلى صورة رقمية مشفرة وتتكون المعلومات النهائية التي تكون جاهزة بعدها للإرسال من دالة رقمية خاصة بالمعلومات ودالة أخرى خاصة بالتوقيع بواسطة المفتاح الخاص وباندماجهما معا ينشأن التوقيع الرقمي ويقوم مستلم المعلومات باستخدام المفتاح العام الذي بحوزته بفك شفرة المعلومات المرسلة[75]، وهناك نوعان للتوقيع وهما كالتالي[76]:

أ- التوقيع المفتاحي Key-Based signature:

يقوم هذا النوع بتزويد الوثيقة الإلكترونية بتوقيع مميز يحدد خلاله الشخص الذي قام بالتوقيع ووقت التوقيع ومعلومات هامة عن صاحب التوقيع، حيث يتم تسجيل التوقيع الرقمي بشكل رسمي عند جهات خاصة تعرف باسم Certification Authority وهو طرف محايد مهمته التأكيد من صحة ملكية التوقيع الرقمي.

ب- التوقيع البيومتري Biometrics Signature:

هو عبارة عن تحديد نمط معين لحركة يد الشخص الذي يقوم بالتوقيع وذلك من خلال توصيل القلم الإلكتروني المستخدم في التوقيع بجهاز حاسب آلي يقوم

الشخص باستخدامه للتوقيع ومن خلال الصلة بين القلم والحاسب الآلي يقوم بتسجيل حركة اليد عند التوقيع، حيث إن حركة اليد أثناء التوقيع تختلف بين شخص وآخر وهي من السمات الشخصية التي لا تتكرر، ويتم تسجيل التوقيع البيومتري من خلال جهة محايدة كالتي تستخدم في التوقيع المفتاحي.

8- العلامات المائية Digital Watermarking:

تستخدم هذه العلامات في كثير من الأحيان كطريقة لضمان ملكية المحتوى وقد تكون العلامات عن نص مرئي أو شعار يحدد بوضوح المالك الحقيقي للمصنف وتكون هذه العلامات بتغطية جزء كبير من البيانات ويصعب إزالتها، وبعض هذه العلامات غير مرئية للعين البشرية ويمكن استرداد هذه البيانات بعد موافقة المالك للمصنف حتى يقوم بإزالة العلامات المائية من المصنف ويكون بعدها صالحا للاستخدام[77].

رابعا: التدابير التشريعية Legal Measures:

نتيجة لإساءة استخدام التقنيات التكنولوجية الحديثة باستخدام الحاسب الآلي وخدمات الإنترنت، بادرت العديد من الدول باتخاذ العديد من التدابير التشريعية ضد هذه المخاطر، سنتناول فيما يلي أهم التدابير التشريعية التي تحمي أمن المعلومات على المستوى الدولي بالإضافة إلى أحدث التشريعات التي صدرت في جمهورية مصر العربية بشأن حماية أمن المعلومات من المخاطر التي تستخدم تقنيات المعلومات وذلك على النحو التالي:

1. التدابير التشريعية الدولية:

تعد معاهدة الويبو بشأن حماية حق المؤلف 1996 ومعاهدة الويبو بشأن فناني الأداء والتسجيلات الصوتية 1996 ويطلق عليهما اتفاقيتي الإنترنت من أولى الجهود الدولية التي تناولت إشكالية حماية أمن المعلومات في بيئة الإنترنت لأنهما

توفران الحماية لحقوق المؤلف والحقوق المجاورة في بيئة الإنترنت، حيث حرصت معاهدة الويبو بشأن حق المؤلف في المادة الرابعة على تأكيد أن برامج الحاسب الآلي تعتبر من المصنفات الأدبية، وأيضاً في المادة الثامنة منها نصت على حماية المصنفات الرقمية التي تنشر على شبكة الإنترنت[78].

كما جاءت اتفاقية بودابست للجرائم الإلكترونية 2001 حيث اهتمت بجرائم الفضاء الإلكتروني ولا سيما الجرائم المرتكبة من خلال استخدام تكنولوجيا الاتصالات وخدمات الإنترنت مثل الجرائم المتعلقة بالمعاملات المالية غير المشروعة وانتهاك حقوق التأليف والنشر بالإضافة إلى تناولها للجرائم التي تنتهك كرامة الإنسان وخصوصيته[79].

وتضمنت اتفاقية بودابست العديد من صور الجرائم الإلكترونية بما في ذلك الجرائم المرتكبة ضد انتهاك العناصر الأساسية لأمن المعلومات وهي السرية وسلامة وتوافر البيانات، أي أن هذه الاتفاقية اهتمت بحماية أمن المعلومات وذلك عن طريق فرض الحماية على عناصرها أو ما يسمى بمثلث CIA.

فقد كانت أول التشريعات التي تستخدم مصطلح نظم الحساب الآلي Computer Systems ووضع تعريف مفصل له في نصوص الاتفاقية هو أي جهاز يقوم بالمعالجة التلقائية للبيانات أو مجموعة من الأجهزة المترابطة أو ذات صلة ببعضها البعض، وبهذا المفهوم فإن الاتفاقية قد شملت كل الأجهزة الرقمية بما فيها ما أطلق عليه فيما بعد بإنترنت الأشياء Internet of Things (IoT)[80].

بالإضافة إلى اتفاقية بودابست فقد أصدر الإتحاد الأوروبي تشريع خاص بأمن الشبكات والمعلومات في عام 2016 يسمى بتوجيه الاتحاد الأوروبي لأمن الشبكات والمعلومات Network and Information Security (NIS) Directive الذي اهتم بحماية عناصر أمن المعلومات CIA، ويعد أول تشريع على مستوى الإتحاد الأوروبي بشأن أمن

الفضاء الرقمي الذي يحمل رقم 169 وتتمثل أهدافه في تحقيق الحد الأقصى من حماية البيئة الإلكترونية وتحديد العلاقة بين مزودي خدمات الإنترنت والمستخدمين وعلاقتهما معاً بالأمن المعلوماتي على مستوى الإتحاد الأوروبي[81].

2. التدابير التشريعية الوطنية:

يعتبر قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 من أحدث التشريعات الوطنية في حماية جرائم تقنيات المعلومات وذلك لاشتماله على العديد من صور الجرائم التي تتم في بيئة الإنترنت والنص على العقوبات التي تقع على مرتكبي مثل هذه الجرائم وكذلك تحديد العلاقة التي تربط مزودي خدمات الإنترنت بالمستخدم لهذه الخدمة والتزامات كلٍ منهم حتى لا يقع تحت طائلة القانون.

تضمن القانون العديد من الصور للجرائم مثل الاعتداء على سلامة شبكات الإنترنت وتقنيات المعلومات وجرائم الدخول غير المشروع واعتراض البيانات بدون وجه حق، حيث نص في المادة 16 على عقوبة الحبس مدة لا تقل عن سنة وغرامة ماليه لا تقل عن خمسين ألف جنية ولا تتجاوز مائتين وخمسين ألف جنية لكل من اعترض بوجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة الإنترنت أو أحد أجهزة الحاسب الآلي[82].

بالإضافة إلى التأكيد على حماية عناصر أمن المعلومات CIA حيث نصت في المادة 17 على العقوبة بالحبس مدة لا تقل عن سنتين وغرامة لا تقل عن مائة ألف جنية ولا تجاوز خمسمائة ألف جنية كل من أتلف أو عطل أو عدل مسار أو ألغى متعمداً وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلفة على أي نظام معلوماتي وما في حكمة أيا كانت الوسيلة التي استخدمت في الجريمة[83].

نشير إلى أن قانون مكافحة جرائم تقنية المعلومات المصري قد نص على جرائم أخرى تهدد أمن المعلومات مثل جرائم الاعتداء على البريد الإلكتروني وجرائم الاعتداء على تصميم المواقع الإلكترونية وجرائم الاعتداء على الأنظمة المعلوماتية وتهديد سلامتها مع توقيع أقصى العقوبة على من قام بواحدة من تلك الجرائم سواء بالحبس أو بالغرامة المالية أو بإحدى العقوبتين.

المعايير الدولية لإدارة أمن المعلومات:

تعتبر المنظمة الدولية للتوحيد القياسي International Organization for Standardization (ISO) التي تعرف باسم منظمة الأيزو هي المنظمة التي تهتم بوضع المعايير الدولية لضبط أمن المعلومات بالمؤسسات والمنظمات، وهي منظمة تضم ممثلين من عدة منظمات قومية للمعايير وبالرغم من أنها منظمة غير حكومية إلا أن المعايير التي تقوم بوضعها تعتبر بمثابة قوانين واجبة التطبيق هذا ما يجعلها أكثر قوة من معظم المنظمات غير الحكومية[84]، وتقع منظمة الأيزو في مدينة جنيف حيث تم تأسيسها عام 1946 وتضم أكثر من 145 بلد عضو منذ إنشائها، وبلغ عدد المعايير الدولية التي أصدرتها 19500 معيار[85].

وترتكز المعايير الدولية على مجموعة من الإجراءات التي يقترح تطبيقها في مؤسسات المعلومات والاعتماد عليها، وأصدرت منظمة الأيزو العديد من المواصفات القاسية المتخصصة في مجال أمن المعلومات نذكر منها معايير ISO, MEHARI, ITIL, COBIT[86]، وأهم هذه المعايير التي تسمى بمواصفات نظم إدارة أمن المعلومات (ISO:27000)، وتتكون من ستة معايير فرعية، وهما كما يلي[87]:

1. أيزو 27001: يشتمل على المعايير الخاصة بالاستمرار على تحسين الخدمات عن طريق وضع الأسس اللازمة لضبط ممارسات الأفراد في إدارة أمن المعلومات.

2. أيزو 27002: يعطي المبادئ والمعايير الخاصة بتنظيم وإدارة أمن المعلومات.
3. أيزو 27003: يوفر القواعد الخاصة بتنفيذ الإجراءات الإضافية الخاصة بأمن المعلومات.
4. أيزو 27004: يهتم توفير المقاييس الخاصة بقياس مدى فعالية تطبيق نظم إدارة أمن المعلومات من خلال مجموعة من الضوابط والمواصفات.
5. أيزو 27005: يوفر مجموعة من المقاييس الخاصة بإدارة المخاطر التي تهدد أمن المعلومات.
6. أيزو 27006: يقدم مبادئ وضوابط توجيهية للاعتماد بالمنظمات التي تقدم الشهادات الخاصة بالمصادقة على نظام إدارة أمن المعلومات.

نوضح فيما يلي أهم هذه المعايير وأكثرها تطبيقاً في إدارة نظم أمن المعلومات وهما معيارا الأيزو 27001 و27002 وذلك على النحو التالي:

1- المعيار الدولي لأمن المعلومات ISO 27001:

صدر هذا المعيار في عام 2005 وهو عبارة عن مجموعة من الإرشادات والإجراءات المتبعة لتطوير وتشغيل ومراقبة ومراجعة وتحسين نظام أمن المعلومات الموثق داخل المنظمة بهدف تحقيق الإدارة الفعالة والمستمرة للمخاطر التي تتعرض لها أمن المعلومات مع توفير الحماية المناسبة لها، وضمان وضع إطار رقابي حازم من خلال إنشاء نظام لإدارة المعلومات والالتزام بالمتطلبات التي يحققها[88].

يهدف هذا المعيار إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل واستراض وصيانة وتحسين نظام إدارة أمن المعلومات داخل المنظمات وعادة ما يصلح للتطبيق على جميع أنواع المنظمات بما في ذلك المنظمات ذات النشاط

التجاري أو الأنظمة الحكومية بفروعها المختلفة، حيث يعتمد هذا المعيار على نموذج يعرف بدائرة ديمنج أو نموذج التحسين المستمر للأداء Plan-Do-Check-Act (PDCA) الذي يتكون من أربع مراحل متتالية تمثل أحد أهم آليات إدارة الأعمال وتطوير الجودة بالمؤسسات وهي[89]:

- مرحلة التخطيط Plan: تأسيس نظام لإدارة أمن المعلومات.
- مرحلة التنفيذ Do: تنفيذ الخطط وتشغيلها.
- مرحلة التحقق Check: مراجعة النظام بعد تنفيذه وتشغيله.
- مرحلة العمل Act: صيانة وتحسين أداء وكفاءة النظام.

2- المعيار الدولي لأمن المعلومات ISO 27002:

يطلق على هذا المعيار "قواعد ممارسة إدارة أمن المعلومات" وهو أول معيار يصدر عن سلسلة معايير إدارة أمن المعلومات (أيزو 27000) الصادرة عن المنظمة الدولية للتوحيد القياسي، ويهدف هذا المعيار إلى توفير القواعد والمواصفات التي تضبط منهجية إدارة أمن المعلومات من خلال الاسترشاد بأفضل الممارسات الأمنية التي من شأنها أن تساعد في الوصول إلى الحد الأدنى لأمن المعلومات[90].

وصدر هذا المعيار في عام 2013 لمواكبة التطورات في أمن المعلومات وتكنولوجيا الاتصالات فهو يوفر إرشادات حول الممارسات الواجب إتباعها في اختيار وتنفيذ وإدارة أمن المعلومات حيث تم إعداده وتصميمة ليتم استخدامه كمرجع لمعرفة الإرشادات والإجراءات الواجب إتباعها لإدارة نظم أمن المعلومات إلى جانب المواصفات والخطوات الإرشادية الواردة بمعيار الأيزو 27001:2013[91].

النتائج والتوصيات:

النتائج:

من خلال البحث في أمن المعلومات الرقمية وتتبع المخاطر التي يتعرض لها، خرجت الدراسة بعدة نتائج هامة يمكن إيجازها في النقاط التالية:

1. ظهور الجانب السلبي لانتشار خدمات الإنترنت مع ظهور العديد من الجرائم الإلكترونية وصعوبة حصرها.
2. يتعرض أمن المعلومات للعديد من المخاطر والتهديدات التي تتم في بيئة الإنترنت مع عدم مواكبة التدابير التقنية المضادة لسرعة تطور الطرق الحديثة المستخدمة في عمليات الاعتداءات على أمن المعلومات.
3. ضعف التشريعات الموجودة على أرض الواقع سواء على المستوى الوطني أو الدولي مع وجود بطء ملحوظ في العمل على كفاية التشريعات الموجودة للحد من عمليات التعدي على أمن المعلومات.
4. قلة خبرة العاملين داخل المنشآت المعلوماتية مما يؤدي إلى حدوث مخاطر من داخل النظام نفسه والعاملين فيه ويساعد ذلك على ظهور جرائم الاحتيال والهندسة الاجتماعية.
5. قلة خبرة مستخدم الإنترنت نفسه في التعامل مع الوسائل التي يستخدمها المهاجمون.
6. التطور السريع للأساليب والتقنيات المستخدمة في الجرائم الإلكترونية مما يصعب من مهمة شركات البرمجيات المضادة للفيروسات، ووضع ضغوط مستمرة على الهيئات التشريعية.

7. إن القوانين المتبعة في حماية أمن المعلومات الرقمية تبطئ من عمل المديرين في أمن المعلومات لعدم مواكبتها للأساليب الحديثة المتبعة في الهجمات الإلكترونية لأنها ليست فعاله بالشكل الكافي، وتفتقر إلى آلية التطبيق نظراً لتنوع هذه الهجمات وتطورها المستمر.

التوصيات:

خرجت الدراسة بعدة توصيات من خلال دراسة أمن المعلومات من الجانب التقني في البيئة الرقمية وما تتعرض له من جرائم بالإضافة إلى دراسة بعض التدابير اللازمة للحد من هذه الجرائم، وهي كالتالي:

1. ضرورة تدريب العاملين داخل نظام أمن المعلومات والقيام بالعديد من الدورات التي تنمي مهاراتهم وقدراتهم المعرفية والتقنية في مجال أمن المعلومات.
2. ضرورة القيام بدورات لتوعية المستخدمين أنفسهم على حماية بياناتهم الشخصية على الإنترنت.
3. العمل على ملاحقة التطورات التي تظهر في أساليب وتقنيات الجرائم الإلكترونية عن طريق عمل برمجيات مضادة للحد من هذه الجرائم.
4. ضرورة تطوير التشريعات الخاصة بأمن المعلومات بشكل مستمر على المستويين الوطني والدولي لمعاقبة مرتكبي مثل هذه الجرائم والعمل على ردع من يقوم بمثل هذه الاعتداءات.
5. ضرورة توحيد الجهود على المستوى الدولي لعمل تشريع موحد يظهر فيه بشكل واضح العقوبات المناسبة لمرتكبي جرائم المعلومات.

6. العمل على تعاون تشريعي وثقافي على المستوى العربي للوقوف سوياً ضد الجرائم التي ترتكب في بيئة الإنترنت.
7. وأخيراً ضرورة وضع تشريع عربي موحد يلتزم به المستخدم العربي لمعرفة العقوبات التي تطاله في حالة وجود النية في القيام بأي عمل من شأنه إحداث تهديدات واضحة على أمن المعلومات.

قائمة المصادر:

(1) Internet World State. World Internet Users and Population Stats 2018, Available At: https://www.internetworldstats.com/stats.htm, Access Date: (27/3/2019).

(2) Internet World State. Arabic Speaking Internet Users Statistics 2018, Available At: https://www.internetworldstats.com/stats19.htm, Access Date: (27/3/2019).

(3) نورة شلوش. القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعدة لأمن الدول، مجلة بابل للدراسات الإنسانية، مج8، ع2، 2018، ص192، متاح على: https://search.mandumah.com/Record/896052، تاريخ الاطلاع: (2019/3/27).

(4) محمد الحسن. القرصنة الإلكترونية تاريخ من الأخطار، مجلة التقدم العلمي، 2017، ص35، متاح على: http://www.kfas.org/media/Taqaddum202017.pdf، تاريخ الاطلاع: (2019/3/28).

(5) MacAfee. Economic Impact of Cybercrime: No Slowing Down, 2018, Available At: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf, Access Date: (1/4/2019).

(6) Grant Gross. The Cost of Cybercrime, Internet Society 2018, Available At: https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime, Access Date: (1/4/2019).

(7) فتيحه رصاع. الجريمة المعلوماتية، مجلة فكر وإبداع، ج101، 2016، متاح على: https://search.mandumah.com/Record/772734، تاريخ الاطلاع: (2019/3/28).

(8) **Tony Campbell. Practical Information Security Management, Berlin: Springer International Publishing Ag, 2016, P.14, Available At: http://link.springer.com/10.1007/978-1-4842-1685-9, Access Date: (30/3/2019).**

(9) شعبان عبد العزيز خليفة. تشريعات الكتب والمكتبات والمعلومات المعاصرة، القاهرة: الدار المصرية اللبنانية، 1997. ص25.

(10) عزة فاروق جوهري. الميتاداتا ودعم استرجاع المحتوى الرقمي للصحف العربية الإلكترونية في البيئة الرقمية: دراسة تطبيقية لمدى تمثيلها في بعض الصحف المصرية والسعودية، مجلة بحوث في علم المكتبات والمعلومات، مركز بحوث نظم وخدمات المعلومات، كلية الآداب، جامعة القاهرة، ع7، 2011، ص50، متاح على: https://search.mandumah.com/Record/708207، تاريخ الاطلاع: (2019/4/3).

(11) أسامة محمد عطية خميس. المحتوى الرقمي في المستودعات الرقمية في البلاد العربية على شبكة الإنترنت: دراسة استطلاعية، الاتجاهات الحديثة فثي المكتبات والمعلومات، مج19، ع37، 2012، ص312.

(12) أسامة أحمد بدر. تداول المصنفات عبر الإنترنت (مشكلات وحلول)، دار الجامعة الجديدة للنشر، الإسكندرية، 2006، ص72.

(13) أيهاب محمد لطفي نور الدين. أثر الإسناد الخارجي لمهام تكنولوجيا المعلومات على أمن وسرية المعلومات، مصر: جامعة عين شمس، معهد الدراسات والبحوث البيئية، قسم العلوم الاقتصادية والقانونية والإدارية البيئية، (أطروحة ماجستير)، 2018.

(14) عبد الوهاب ملياني. أمن المعلومات في بيئة الأعمال الإلكترونية، الجزائر: جامعة أبي بكر بلقايد، كلية الحقوق والعلوم السياسية، أطروحة دكتوراه)، 2017.

(15) معاذ أحمد عبد الرازق. أمن المعلومات ودوره في الحد من القرصنة الإلكترونية، المركز القومي للمعلومات: دراسة حالة، السودان: جامعة أم درمان الإسلامية، معهد بحوث ودراسات العالم الإسلامي، (أطروحة ماجستير)، 2016.

(16) منال بنت حمدان بن سعيد العميري. واقع ممارسات أمن المعلومات في المكتبة الرئيسية بجامعة السلطان قابوس ومدى توافقها مع المعيار الدولي لأمن المعلومات **(ISO/IEC 27002)**: دراسة حالة، عمان: جامعة السلطان قابوس، كلية الآداب والعلوم الاجتماعية، (أطروحة ماجستير)، 2016.

(17) Venessa Burton Howard. Protecting small business information from cyber security criminals: A qualitative study, United States: Colorado Technical University, Management Dep. (PhD), 2018, Available at: https://search.proquest.com/docview/2133581243?accountid=178282, Access Date: (12/4/2019).

(18) **Ibrahim Ghafir, Jibran Saleem, Mohammad Hammoudeh… et al. Security Threats to Critical Infrastructure: The Human Factor, The Journal of Supercomputing, Vol. 74, No. 10, USA: Springer, Gross Mark, 2018, Available At: https://link.springer.com/article/10.1007%2Fs11227-018-2337-2, Access Date: (13/4/2019).**

(19) **Michele Zoerb. Information Security Program Framework, United States: Utica College, Cybersecurity Dep, (Master), 2017, Available At: https://search.proquest.com/docview/1978088529?accountid=178282, Access Date: (12/4/2019).**

(20) **Rolf H. Weber, Evelyne Studer. Cybersecurity in the Internet of Things: Legal Aspects, Computer Law & Security Review, Vol. 32, No. 5, Switzerland:**

Elsevier, 2016, Available At: https://www.sciencedirect.com/science/article/pii/S0267364916301169?via%3Dihub, Access Date: (14/4/2019).

(21) John M. Broky, Thomas H. Bradley. Protecting Information with Cybersecurity, Berlin: Springer International Publishing AG, 2019, Pp. 350-351, Available At: http://08102q3xn.1104.y.https.link.springer.com.mplbci.ekb.eg/content/pdf, Access Date: (15/4/2019).

(22) Ibid. P. 347.

(23) Sagar Ajay Rahalkar. Certified Ethical Hacker (CEH) Foundation Guide: Information Security Basic, India: Press, 2016, P. 91, Available At: https.link.springer.com.mplbci.ekb.eg/content/pdf/10.1007%2F978-1-4842-2325-3.pdf, Access Date: (1/4/2019).

(24) رجب عبد الحميد حسنين. أمن شبكات المعلومات والمكتبات: المخاطر والحلول، Cybrarians Journal، ع30، 2012، متاح على: http://www.journal.cybrarians.org/index.php?option=com_content، تاريخ الاطلاع: (2019/4/14).

(25) معاذ يوسف الذنيبات، خلف محمود البقور، فتح الرحمن محمد يوسف. مخاطر أمن المعلومات في تطبيقات الحكومة الإلكترونية وأثرها في كفاءة نظام المعلومات، مجلة البحوث التجارية المعاصرة، مج28، ع2، جامعة سوهاج: كلية التجارة، 2014، ص404، متاح على: http://search.mandumah.com/Record/676415، تاريخ الاطلاع: (2019/4/14).

(26) John M. Broky, Thomas H. Bradley. Op. Cit, P. 347.

(27) أمنية قدايفة. استراتيجية أمن المعلومات، مجلة أبعاد اقتصادية، مج6، ع1، الجزائر، 2016، ص ص167-168، متاح على: https://www.asjp.cerist.dz/en/downArticle/279/6/1/31120، تاريخ الاطلاع: (2019/4/15).

(28) **John M.D. Hunter. An Information Security Handbook, London: Springer, 2010, P. 7, Available At: http://08102olk6.1103.y.https.link.springer.com.mplbci.ekb.eg/content/pdf , Access Date: (17/4/2019).**

(29) معاذ يوسف الذنيبات. مخاطر أمن المعلومات المحتملة في تطبيقات التعاملات الإلكترونية وأثرها في كفاءة نظام المعلومات، مجلة البحوث الأمنية، مج24، ع60، 2015، ص ص25-26، متاح على: http://search.mandumah.com/Record/653335، تاريخ الاطلاع: (2019/4/15).

(30) أشرف عبد المحسن الشريف. أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية، مجلة الاتحاد العربي للمكتبات والمعلومات (اعلم)، ع16، 2016، ص98، متاح على: https://search.mandumah.com/Record/702627، تاريخ الاطلاع: (2019/4/17).

(31) معاذ أحمد عبد الرازق أحمد. مصدر سابق، ص30.

(32) أمنية قدايفة. مصدر سابق، ص168.

(33) فادية عبد الرحمن خالد. سياسة أمن المعلومات في المكتبات ومراكز المعلومات، المجلة الأردنية للمكتبات والمعلومات، مج52، ع4، 2017، ص74، متاح على: http://content.ebscohost.com/ContentServer.asp، تاريخ الاطلاع: (2019/4/17).

(34) **Gattiker Urs E. The Information Security: Defining the Terms That Define Security for E-Business, Internet, Information and Wireless Technology, New**

York: Kluwer Academic Publishers, 2015, P. 91, Available At: http://08102olk6.1103.y.https.link.springer.com.mplbci.ekb.eg, Access Date: (7/4/2019).

(35) Sagar Ajay Rahalkar. Op. Cit, P. 123.

(36) Ibrahim Ghafir, Op. Cit, P. 4.

(37) Chinese Academy of Cyberspace Studies. Improving Capacity of Cyber Security Safeguarding in Chinese Academy of Cyberspace, Berlin: Springer, 2019, P. 103, Available At: http://08102q3xn.1104.y.https.link.springer.com.mplbci.ekb.eg/content/pdf, Access Date: (12/4/2019).

(38) Theodoros T., Loukas K. Online Social Network Phishing Attack, Encyclopedia of Social Network Analysis and Mining, New York: Springer, 2018, P. 38, Available At: https://link.springer.com/content/pdf/10.1007%2F978-1-4939-7131-2_348.pdf, Access Date: (13/4/2019).

(39) معاذ يوسف الذنيبات، خلف محمود البقور، فتح الرحمن محمد يوسف. مصدر سابق، ص405.

(40) Rolf H. Weber, Evelyne Studer. Op. Cit, P. 717.

(41) Javier Martinez Torres, Carla Iglesias Comesana, Paulino J. Garcia-Nieto. Review: Machine Learning Techniques Applied to Cybersecurity, Germany: Springer-Verlag GmbH, 2019, P. 6, Available At: http://08102qrbe.1104.y.https.link.springer.com.mplbci.ekb.eg, Access Date: (14/4/2019).

(42) Fernando Georgel Birleanu Peter Anghelescu, Nicu Bizon. Malicious and Deliberate Attacks and Power System Resiliency, Switzerland: Springer Nature AG, 2019, P. 230, Available At: http://08102qrbe.1104.y.https.link.springer.com.mplbci.ekb.eg/content/pdf , Access Date: (15/4/2019).

(43) Kang Leng Chiew, Kalvin Sheng Chek Yong, Choon Lin Tan. A Survey of Phishing Attacks: Their Types, Vectors and Technical Approaches, Expert Systems with Applications, Vol. 106, Malaysia: Elsevier Ltd, 2018, P. 7, Available At: https://08101xhed-1105-y-https-ac-els--cdn-com.mplbci.ekb.eg, Access Date: (15/4/2019).

(44) معاذ أحمد عبد الرازق أحمد. مصدر سابق، ص50.

(45) Javier Martinez Torres, Carla Iglesias Comesana, Paulino J. Garcia-Nieto. Op. Cit. P. 6.

(46) Leila Benarous, Benamar Kadri, Ahmed Nouridane. A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions, 2017, P. 10, Available At: https://link.springer.com/content/pdf/10.1007%2F978-3-319-47301-7_15.pdf, Access Date: (15/4/2019).

(47) Nihad A. Hassan, Rami Hijazi. Introduction to Online Threats and Countermeasures, Open Source Intelligence Methods and Tools, California: Apress, Berkeley, CA, 2018, P. 29, Available At: http://08102xj8q.1105.y.https.link.springer.com.mplbci.ekb.eg/content/pdf , Access date: (16/4/2019).

(48) **Bettany A., Halsey M. What Is Malware? Windows, Virus and Malware Troubleshooting, California: Apress, Berkeley, CA, 2017, P. 4, Available At: http://08102xj8u.1105.y.https.link.springer.com.mplbci.ekb.eg/content/pdf , Access Date: (16/4/2019).**

(49) **Shailendra Rathore, Pradip Kumar Sharma. Social network security: Issues, challenges, threats, and solutions, Information Sciences, Vol 421, Italy: Elsevier Ltd, 2018, P. 51, Available At: https://08101nknm-1103-y-https-ac-els--cdn-com.mplbci.ekb.eg, Access Date: (16/1/2019).**

(50) **Ibid, P. 10.**

(51) كمال محمود جبرا. التأمين وإدارة الخطر، القاهرة: الأكاديميون للنشر والتوزيع، 2015، ص122.

(52) عماد أحمد محمد. إدارة وتحليل مخاطر أمن المعلومات، مؤتمر أمن المعلومات والحكومة الإلكترونية، ماليزيا: المنظمة العربية للتنمية الإدارية، 2009، ص17، متاح على: http://search.mandumah.com/Record/121050، تاريخ الاطلاع: (2019/4/20).

(53) أشرف عبد المحسن الشريف. مصدر سابق، ص102.

(54) حسين علي قاسم الشمالي. أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن، الأردن: جامعة اربد، 2016، ص193، متاح على: https://dspace.qou.edu/bitstream/194/1574/2/380-1457-1-CE.pdf، تاريخ الاطلاع: (2019/4/20).

(55) المصدر سابق، ص ص192-193.

(56) **Alice Hutchings, Russell G. Smith, Lachlan Hames. Criminals in the Cloud: Crime, Security Threats, and Prevention Measures, Switzerland: Palgrave**

Macmillan, 2015, P. 158, Available At:
https://link.springer.com/content/pdf/10.1057%2F9781137474162_10.pdf, Access Date: (18/4/2019).

(57) أسامه بن غانم العبيدي. جريمة الدخول غير المشروع إلى النظام المعلوماتي: دراسة قانونية في ضوء القوانين المقارنة، مجلة دراسات المعلومات، ع14، السعودية: جمعية المكتبات والمعلومات، 2012، ص27، متاح على:
https://search.mandumah.com/Record/206884، تاريخ الاطلاع: (2019/4/6).

(58) معاذ أحمد عبد الرازق أحمد. مصدر سابق، ص57.

(59) صحوه صلاح عبد الرازق. التخطيط الاستراتيجي لأمن المعلومات، (أطروحة ماجستير)، جامعة أم درمان: معهد البحوث والدراسات الاستراتيجية، 2017، ص35، متاح على:
http://search.mandumah.com/Record/858537، تاريخ الاطلاع: (2019/4/21).

(60) **Nihad A. Hassan, Rami Hijazi. Op. Cit, P. 31.**

(61) محمد محمد الألفي. الحماية القانونية لقواعد البيانات في نظم المعلومات، القاهرة: المنظمة العربية للتنمية الإدارية، 2010، ص 191، متاح على:
https://search.mandumah.com/Record/125070، تاريخ الاطلاع (2019/4/21).

(62) نوفل حديد، مسوس كمال. مقاربات حماية أنظمة معلومات المؤسسة من الاعتداءات الإلكترونية، مرجع سابق، ص37.

(63) سعد عبد السلام طلحة، أحمد نوري. مصدر سابق، ص24.

(64) **Qiuyan Tian, Hao Kang, Ting Ai. Analysis and Comparison of Network Information Security Encryption Technology, Advanced in Engineering, Vol. 166, China: Atlantis Press, 2018, P. 679, Available At:**

https://download.atlantis-press.com/article/25895751.pdf, Access Date: (11/4/2019).

(65) عادل عثمان جابر. مصدر سابق، ص22.

(66) المصدر السابق، ص23.

(67) أسامه بن غانم العبيدي. مصدر سابق، ص25.

(68) Richard Stanley. Information Security, Cybercrimes: A Multidisciplinary Analysis, Berlin: Springer, 2011, P. 117, Available At: https://link.springer.com.mplbci.ekb.eg/content/pdf, Access Date: (12/4/2019).

(69) John M. Broky, Thomas H. Bradley. Op. Cit, P. 383.

(70) رجب عبد الحميد حسنين، مصدر سابق.

(71) فاتن سعيد باملفح. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى، مجلة الاتجاهات الحديثة في المكتبات المعلومات، مج9، ع18، 2002، ص255، متاح على: http://ethraadl.com:809/upload/4351.pdf، تاريخ الاطلاع: (2019/4/22).

(72) Hisham Al-Assam, Waleed Hassan, Sherali Zeadally. Automated Biometrics Authentication with Cloud Computing, Biometric-Based Physical and Cybersecurity Systems, Switzerland: Springer Nature, 2019, P. 459, Available At: http://081020lva.1105.y.https.link.springer.com.mplbci.ekb.eg, Access Date: (17/4/2019).

(73) Ibid. P. 460.

(74) أشرف عبد المحسن الشريف، مصدر سابق، ص ص106-107.

(75) صحوه صلاح عبد الرازق. مصدر سابق، ص35.

(76) أحمد عبد الله مصطفى. حقوق الملكية الفكرية والتأليف في بيئة الإنترنت، البوابة العربية للمكتبات والمعلومات **Cybrarians Journal**، ع21، 2009، ص ص19-20، متاح على: **http://search.mandumah.com/Record/507991**، تاريخ الاطلاع: (2019/4/21).

(77) **Shailendra Rathore, Pradip Kumar Sharma. Op. Cit, P. 54.**

(78) المصدر سابق، ص22.

(79) مجلس أوروبا. التقرير التفسيري لاتفاقية الجريمة الإلكترونية، سلسلة المعاهدات الأوروبية (185)، ص3، متاح على: **https://rm.coe.int/explanatory-report-budapest-convention-in-arabic**، تاريخ الاطلاع: (2019/4/23).

(80) **Rolf H. Weber, Evelyne Studer. Op Cit, P. 722.**

(81) **Ibid. P.723.**

(82) الجريدة الرسمية. قانون رقم 175 لسنة 2018 بشأن حماية جرائم تقنية المعلومات، ع32 مكرر (ج)، 2018، ص14، متاح على: **https://alborsaanews.com/app/uploads/2018/08/1534588973_279_342416.pdf**، تاريخ الاطلاع: (2019/4/22).

(83) المصدر السابق، ص15.

(84) أحمد عبادة العربي. معيار المنظمة الدولية للتوحيد القياسي أيزو 27002 لسياسات أمن المعلومات: دراسة وصفية تحليلية لمواقع الجامعات المصرية، مجلة جامعة طيبة للآداب والعلوم الإنسانية، مج4، ع7، ص663، متاح على: **http://search.mandumah.com/Record/773513**، تاريخ الاطلاع: (2019/4/22).

(85) **Paul de Hert, Vagelis Papakonstantinou, Irene Kamara. The Cloud Computing Standard ISO/IEC 27018 Through the Lens of The EU Legislation**

on Data Protection, Computer Law & Security Review ،Vol. 32, Belgium: Elsevier Ltd, 2016, P. 17, Available At: https://081010y1y-1105-y-https-ac-els--cdn-com.mplbci.ekb.eg, , Access Date: (19/4/2019).

(86) نوفل حديد، مسوس كمال. مصدر سابق، ص38.

(87) **MacLennan A. Information Governance and Assurance, International Journal of Information Management, Vol. 35, London: Elsevier Fact Publisher, 2015, P. 174, Available At: https://081010y2c-1105-y-https-ac-els--cdn-com.mplbci.ekb.eg, Access Date: (19/4/2019).**

(88) إلهام يحياوي، الصديق أبن بوزة. أهمية ودور المواصفة القياسية الأيزو 27001-2005 في مراكز نظم المعلومات الجغرافية: دراسة حالة عن بعض الدول العربية، مجلة الاجتهاد للدراسات القانونية والاقتصادية، ع5، الجزائر: المركز الجامعي، 2014، ص223، متاح على: https://search.mandumah.com/Record/92961، تاريخ الاطلاع: (2019/4/22).

(89) أحمد بن علي عبد الله. رؤية إستراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية، (أطروحة ماجستير)، الرياض: جامعة نايف العربية للعلوم الأمنية، كلية العلوم الإستراتيجية، 2015، ص71، متاح على: https://core.ac.uk/download/pdf/80744102.pdf، تاريخ الاطلاع: (2019/4/19).

(90) منال بنت حمدان بن سعيد العميري. مصدر سابق، ص9.

(91) **Paul de Hert, Vagelis Papakonstantinou, Irene Kamara, Op Cit, P. 23.**