



**المملكة العربية السعودية**

**وزارة التعليم**

**إدارة التعليم بمنطقة**



**بحث عن الحاسب الآلي**

**امن المعلومات**

إعداد الطالبة :

**مقدمة عن أمـــن المعلومات**

 أمن المعلومات ، من زاوية أكاديمية ، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها . ومن زاوية تقنية ، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية . ومن زاوية قانونية ، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها ( جرائم الكمبيوتر والإنترنت) .

واستخدام اصطلاح أمن المعلومات **Information Security**   وان كان استخداما قديما سابقا لولادة وسائل تكنولوجيا المعلومات ، الا انه وجد استخدامه الشائع بل والفعلي ، في نطاق انشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال ، اذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات  وتداولها والتفاعل معها عبر شبكات المعلومات- وتحديدا الإنترنت – احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة

**ما المقصود بأمن المعلومات**

هو فرع من فروع التكنولوجيا المعروفة باسم [أمن المعلومات](https://ar.wikipedia.org/wiki/%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA)، كما هي مطبقة على الحاسوب والشبكات. والهدف من أمن الحاسوب يتضمن حماية المعلومات والممتلكات من السرقة والفساد، أو الكوارث الطبيعية، بينما يسمح للمعلومات والممتلكات أن تبقى منتجة وفي متناول مستخدميها المستهدفين. مصطلحات أمن نظام الحاسوب، تعني العمليات والآليات الجماعية التي من خلالها تٌحمى المعلومات والخدمات الحساسة والقيمة من النشر، والعبث بها أو الانهيار الذي تسببه الأنشطة غير المأذون بها أو الأفراد غير الجديرين بالثقة، والأحداث غير المخطط لها على التوالي.

**عناصر أمن المعلومات**

  **السرية أو الموثوقية  CONFIDENTIALITY**: وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك .

 **التكاملية وسلامة المحتوى INTEGRITY :** التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى او تغيره او العبث به في اية مرحلة من مراحل المعالجة او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات او عن طريق تدخل غير مشروع .

**استمرارية توفر المعلومات او الخدمة AVAILABILITY**  :- التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم  المعلومات لن يتعرض الى منع استخدامه لها او دخوله اليها .

 **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به  Non-repudiation  :-**ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات او مواقعها انكار انه هو الذي قام بهذا التصرف ، بحيث تتوفر قدرة اثبات ان تصرفا ما قد تم من شخص ما في وقت معين .

تهديدات امن المعلومات

الفيروسات

الفيروس هو برنامج صغير مكتوب بأحد للغات الحاسب ويقوم بإحداث أضرار في الحاسب والمعلومات الموجودة على الحاسب بمعني انه يتركز علي ثلاث خواص وهي التخفي، التضاعف، وإلحاق الأذى. مصادر الفيروس يكمن مصادر الفيروس من خلال الرسائل الإلكترونية المجهولة، صفحات الإنترنت المشبوهة، نسخ البرامج المقلدة، استخدام برامج غير موثقة، كذالك تبادل وسائل التخزين دون عمل فحص مسبق مثل الأقراص والذاكرة المتنقلة وإرسال الملفات داخل الشبكة المحلية. للفيروس ثلاث خواص مؤثرة وهي: التضاعف: تتم عملية تضاعف الفيروس عند التحاق الفيروس بأحد الملفات وهنا تتم عملية زيادة عدد العمليات التي تتم إلى ملاين العمليات مما يسبب البطء في العمل أو توقف الحاسب عن العمل. التخفي: لابد للفيروس من التخفي حتى لا ينكشف ويصبح غير فعال، ولكي يتخفي فأنة يقوم بعدة أساليب منها علي سبيل المثال، صغر حجم الفيروس لكي سيناله الاختباء بنجاح في الذاكرة أو ملف آخر. إلحاق الأذى: قد يتراوح الأذى الذي يسببه الفيروس بالاكتفاء بإصدار صوت موسيقي أو مسح جميع المعلومات المخزنة لديك، ومن الأمثلة الاخري في إلحاق الأذى: إلغاء بعض ملفات النظام، إغلاق الحاسب من تلقاء نفسه عند الدخول على الإنترنت مثلا أو إلغاء البرنامج المكتوب على BIOS

هجوم تعطيل الخدمة

وهذا النوع من الخدمة يقوم فيه القرصان أو المعتدي بإجراء أعمال خاصة تؤدي إلى تعطيل الأجهزة التي تقدم الخدمة Server في الشبكات

مهاجمه المعلومات المرسله

وهو اعتراض المعلومات عند ارسالها من جهة إلى أخرى، ويحدث هذا التعامل غالباً أثناء تبادل الرسائل خلال الشبكات: 1. الإنترنت 2. الشبكات التي تستخدم شبكة الهاتف العامة

هجوم السيطرة الكاملة

في هذا النوع يقوم القرصان بالسيطرة الكاملة على جهاز الضحية والتحكم في جميع ملفاتهكما لو كانت في جهازه هو ويمكن للقرصان مراقبة الضحية بصورة كاملة.

يتم الهجوم بعد أن يضع القرصان ملف صغير على جهاز الضحية (عن طريق البريد الإلكتروني أو أي وسيلة أخرى) أو عن طريق استغلال نقاط الضعف في أظمة التشغيل

هجوم التضليل

وفيه يقوم القرصان بانتحال شخصية موقع عام. كما يمكن للقرصان أن ينتحل شخصية مستخدم موثوق به للحصول على معلومات غير مصرحة له

الوصول المباشر لكوابل التوصيل

يقوم المهاجم بالوصول المباشر لأسلاك التوصيل والتجسس على المعلومات المارة. ولكنه هجوم صعب ويتطلب عتاد خاص

**- المقصود  بجرائم تقنية المعلومات:**

**يقصد بجرائم تقنية المعلومات كل فعل غير مشروع يرد على  الكمبيوتر أو يتم باستعماله. كما يُعرفها البعض بأنها كل نشاط إجرامي يؤدي فيه النظام دوراً لإتمامه أو يقع على النظام نفسه.**

**- المجالات المستبعدة من التعاملات الإلكترونية:**

**حرص المنظم في المملكة على استبعاد بعض المجالات من نطاق التعاملات الإلكترونية، وذلك في مجال الأحوال الشخصية وفي مجال التصرفات الواردة على العقارات وذلك لمبلغ خطورتها وتطلب إجراءات رسمية معينة لإبرام هذا  النوع من التعاقدات. لذلك تنص المادة الثالثة من نظام التعاملات الإلكترونية على أنه "يسري هذا النظام التعاملات والتوقيعات الالكترونية ويستثنى من أحكامه ما يلي:**

**1- التعاملات المتعلقة بالأحوال الشخصية**

**2- إصدار الصكوك المتعلقة بالتصرفات الواردة على العقار.**

**وذلك ما لم يصدر من الجهة المسؤولة عن هذه التعاملات ما يسمح بإجرائها الكترونياً، وفق ضوابط تضعها تلك الجهة بالاتفاق مع الوزارة".**

**- مدى الالتزام بإبرام التعاملات الإلكترونية:**

**على الرغم من أن التعاملات الإلكترونية تزداد قبولا في التعاملات بدلا من التعاملات الورقية أو بطريق الفاكس والتليفون، فإن المنظم في المملكة ارتأى ألاّ تكون إجبارية على المتعاملين؛ فيتعين توافر موافقة المتعاملين بها، بشكل صريح أو ضمني، مع استثناء التعامل مع الجهات الحكومية التي يجب أن تكون موافقتها مكتوبة. في ذلك تنص المادة الرابعة من نظام مكافحة جرائم تقنية المعلومات على أنه:**

**"1- لا يلزم هذا النظام أي شخص بالتعامل الالكتروني دون موافقته ويمكن أن تكون هذه الموافقة صريحة أو ضمنية.**

**2- استثناء من الحكم الوارد من الفقرة (1) من هذه المادة، يجب أن تكون موافقة الجهة الحكومية على التعامل الالكتروني صريحة مع مراعاة ما تحدده الجهة الحكومية من اشتراطات للتعامل الالكتروني.**

**3- يجوز لمن يرغب في إجراء تعامل الكتروني ان يضع شروطاً إضافية خاصة به لقبول التعاملات والتوقيعات الالكترونية على الا تتعارض تلك الشروط مع أحكام هذا النظام.".**

**- ضرورة التدخل بالتجريم لحماية التعاملات الإلكترونية:**

        أصبحت خطورة جرائم الحاسب الآلي محل اتفاق بين المتخصصين في علوم القانون وغير المتخصصين، وذلك بالنظر إلى الآثار الخطيرة التي تخلفها تلك الجرائم من الناحية المادية على التعاملات بين الشركات المختلفة وبين الأفراد، بل وبين الأفراد بعضهم ببعض.وتقدر تلك الخسائر بملايين الدولارات. وقد أدى ذلك إلى تهديد سير التجارة الخارجية والداخلية. وقد تعدت خطورة تلك الجرائم اعتبارات التبادلات والصفقات إلى حيز السياسة الدولية حيث إن معظم أسلحة الجيوش يتم تشغيلها بأجهزة الحاسب الآلي.

**كما أنه تبين أن نظام الحاسب الآلي وما يرتبط به من استعمال شبكة الإنترنت له دور إجرامي، أي أنه يسهل ارتكاب أنواع معينة من الجرائم. ومؤدى ذلك أن نظام الحاسب ليس دائما الضحية ولا هو محل للعدوان، بل هو وسيلة الجاني في بعض الأحوال. من ذلك جرائم بث الأفلام والصور المنافية للآداب، أو ارتكاب جرائم ضد أمن الدولة أو ضد الأديان. ومن ذلك أيضا ما تقوم به أنظمة الحاسب من تسهيل جرائم السرقة والنصب والاستيلاء على أموال البنوك وغيرها من الشركات.**

**- أسباب التجريم في مجال تقنية المعلومات:**

**تدوين المعلومات قد يكون على مستندات ورقية وقد يكون في جهاز الكمبيوتر. ولنا أن نتساءل لماذا يتجه الاهتمام نحو البيانات المسجلة في الكمبيوتر دون تلك التي تم تدوينها في مستندات ورقية (فيشات)؟ نرى أن السبب في ذلك يرجع إلى الاعتبارات الآتية:**

**أولاً – كبر حجم السعة الاستيعابية لجهاز الكمبيوتر حيث يسمح الجهاز بتدوين بيانات كثيرة ومتعددة بالمقارنة مع المستندات الورقية.**

**ثانياً – سهولة الرجوع إلى تلك البيانات حيث يتم ذلك بمجرد الضغط على أحد مفاتيح جهاز الكمبيوتر، الأمر الذي لا يتوافر في حالة المستندات الورقية.**

**ثالثاً – إمكانية الدخول إلى النظام عن بعد دون حاجة إلى دخول المكان المتواجد به النظام، أما بالنسبة للإطلاع على المستندات الورقية بدون وجه حق فإنه يقتضي الدخول إلى المكان والتغلب على وسائل الحراسة واستعمال مفاتيح مصطنعة في بعض الأحيان.**

**رابعاً– قد يتم الدخول بوجه حق إلى النظام ابتداءً فينتهز المتهم هذه الفرصة للإطلاع على ملفات أخرى سرية بدون وجه حق.**

**- صور لجرائم تقنية المعلومات:**

**من النصوص الخاصة التي تورد تجريما لحماية تقنية المعلومات تلك التي تعاقب على الدخول  في النظام بدون وجه حق ، وتجريم الإخلال بسير النظام، وتجريم إتلاف البيانات أو العبث بها، وتجريم التنصت أي انتهاك سرية البيانات المبرمجة والتبادلات والمراسلات الإلكترونية.**

**جريمة التنصت على النظام**

**وندرس في هذا  المبحث الأساس القانوني لتجريم التنصت على النظام (في مطلب أول) وأركان تلك الجريمة (في مطلب ثان).**

**المطلب الأول** :**الأساس النظامي لتجريم التنصت على النظام**

**يعاقب النظام السعودي في شأن مكافحة جرائم المعلوماتية على التجسس على النظام بنصه في المادة الثالثة على أن:**

**"يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: 1- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه".**

**المطلب الثاني** :**أركان جريمة التنصت على النظام**

**جريمة التنصت على النظام لها ركنان ؛ركن مادي وركن معنوي على ما سيلي توضيحه؛**

**الفرع الأول** : **الركن المادي لجريمة التنصت على النظام**

**جريمة التنصت على النظام جريمة نشاط وليست جريمة نتيجة، ومن ثمّ فإن الجريمة تقع بنشاط مما هو منصوص عليه في المادة الثالثة من نظام مكافحة جرائم المعلوماتية وهو التنصت أو الالتقاط أو الاعتراض. وعلى الرغم من أن النظام سابق الذكر لم يعرّف المقصود بالتجسس، إلاّ أنه عرف الالتقاط بأنه "مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح"(المادة الأولى – 10).  وعلى أية حال فإن كل هذه الصورتتضمن الاطلاع أو مشاهدة البيانات أو الحصول عليها بأية طريقة أخرى ودون مسوغ قانوني.**

**ويلاحظ أن الصياغة بهذا الشكل لا تغطي إلا التجسس على النظام في أثناء تشغيله، ولا تسري في حالة التجسس على النظام الذي لا يعمل وذلك عن طريق الدخول إليه وتشغيله والاطلاع على محتويات الملفات التي بداخله. ولكن يبقى أن التداخل في حد ذاته يعاقب عليه النظام السعودي ولكن ذلك مشروط بتوافر نية معينة وهي نية التهديد أو الابتزاز أو نية الحصول على بيانات تخص الأمن القومي أو الاقتصاد الوطني أو نية العبث بالبيانات المبرمجة.**

**وتمتد هذه الجريمة لتشمل انتهاك سرية المراسلات الإلكترونية. وهنا يتعين أن نبين  الحدود الفاصلة بين المراسلات الخاصة والمراسلات العامة على شبكة الإنترنت. فهناك الايه ميل وهناك الماسنجر وهي أماكن خاصة، وذلك على عكس المواقع التي يسمح للغير بالدخول إليها ، حتى ولو كان هذا الدخول في مقابل سداد رسم معين أو اشتراك معين.**

**وهنا نؤكد على  ضعف الطابع الخاص للمراسلات بطريق البريد الإلكتروني ، وضرورة إقامة التماثل بين المراسلات الإلكترونية (الإيه ميل) والمراسلات البريدية(****[[15]](http://faculty.ksu.edu.sa/shaimaaatalla/Pages/crifor.aspx%22%20%5Cl%20%22_ftn15%22%20%5Co%20%22)). كما يجب إقامة التماثل بين المحادثات الفورية بطريق الماسنجر والمحادثات الهاتفية في ضرورة حمايتها بعقاب من يتنصت عليها ، الأمر الذي فعله النظام السعودي الجديد.**

**وقد أفرد النظام السعودي نصا خاصا للتجسس على بيانات البنوك بعقابه في المادة الرابعة على "الوصول – دون مسوغ نظامي صحيح- إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات أو معلومات أو أموال أو ما تتيحه من خدمات". وتعاقب المادة الرابعة على ذلك بعقوبة السجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين.**

**الفرع الثاني** :**الركن المعنوي لجريمة التنصت**

**من الواضح أن جريمة التنصت جريمة عمدية فيها ينصرف القصد الجنائي للجاني إلى القيام بالتنصت على نظام أو جهاز الغير لمشاهدة البيانا التي بداخل جهازه أو التقاط ما يرسله جهازه من رسائل. وعلى الرغم من عدم النص صراحة على أن الجريمة عمدية، فإن طبيعة النشاط يقتضي ذلك، حيث إن المشاهدة أو الالتقاط الذي يحدث بطريقة عرضية دون قصد لا يكفي لتوافر صفة التنصت.**

**ويكفي القصد الجنائي العام من توافر العلم والإرادة؛ إرادة النشاط حيث إن  الجريمة من جرائم الخطر. فلا يلزم توافر القصد الجنائي الخاص أي لا يلزم أن تنصرف نية الجاني إلى تحقيق مأرب معين من وراء التنصت؛ فلا يلزم أن يتم من شركة منافسة على أنظمة الشركة الأخرى للتحقيق مكاسب مالية أو غير مالية.**

**مكافحة جرائم تقنية المعلومات عن طريق القواعد الموضوعية والقواعد الإجرائية:**

**وقد كانت تلك الحماية يكفلها القانون عن طريق قواعد موضوعية وقواعد إجرائية، قبل صدور هذا النظام. ونقصد بالقواعد الموضوعية ما توفره النصوص التقليدية في الشريعة الإسلامية والأنظمة الجزائية من تجريم السرقة والنصب وخيانة الأمانة والتزوير، ونقصد بالقواعد الإجرائية تلك التي تنظم جمع الاستدلالات والتحقيق والمحاكمة والتي يعرفها نظام الإجراءات الجزائية في المملكة.**

**وقد أدركت كثير من التشريعات أن القواعد الإجرائية التقليدية غير متلائمة في تطبيقها على الجرائم الإلكترونية، ومن ثم فقد أدخلت قواعد إجرائية جديدة تناسب الاتصالات الإلكترونية. وهذا ما فعله المشرع الأمريكي على وجه الخصوص، على ما سيلي بيانه. ومما يدل على أن القواعد التقليدية الإجرائية غير مناسبة للاتصالات الإلكترونية أن القواعد التي تنظم الاتصالات الهاتفية سواء من ناحية التجريم أو من الناحية الإجرائية يصعب تطبيقها على الاتصالات الإلكترونية.كما أن القواعد التي تنظم المراسلات البريدية لا تناسب في تطبيقها المراسلات الإلكترونية (الإيميل).**

**أهداف نظام مكافحة جرائم تقنية المعلومات في المملكة:**

**أوضح نظام مكافحة جرائم تقنية المعلومات في المملكة أغراض هذا النظام بقوله في المادة الثانية منه "يهدف هذا النظام إلى ضبط التعاملات والتوقيعات الالكترونية، وتنظيمها وتوفير إطار نظامي لها بما يؤدي إلى تحقيق ما يلي:**

**1- إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الالكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بوساطة سجلات الكترونية يعول عليها**

**2- إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الالكترونية وسلامتها**

**3- تيسير استخدام التعاملات والتوقيعات الالكترونية على الصعيدين المحلي والدولي للاستفادة منها في جميع المجالات، كالإجراءات الحكومية والتجارة والطب والتعليم والدفع المالي الالكتروني.**

**4- إزالة العوائق أمام استخدام التعاملات والتوقيعات الالكترونية.**

**5- منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الالكترونية"**

طرق وأدوات لحماية امن المعلومات

التأمين المادي للأجهزة والمعدات.

تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.

تركيب أنظمة كشف الاختراق وتحديثها.

تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية.

عمل سياسة للنسخ الاحتياطي.

استخدام أنظمة قوية لتشفير المعلومات المرسلة.

دعم أجهزة عدم انقطاع التيار.

نشر التعليم والوعي الأمني.

**نتائج وتوصيات البحث**

**- لا تكفي القواعد التقليدية في تجريم السرقة والنصب وخيانة الأمانة والإتلاف والتزوير في مكافحة جرائم تقنية المعلومات**

**- من صور الركن المادي في جريمة الإخلال بالنظام الإعاقة والتأثير في أداء النظام، وقد أحسن النظام السعودي صنعا عندما جرّم الإخلال بسير النظام بالإضافة إلى مسح أو إتلاف أو تعديل البيانات المبرمجة.**

**- أحسن النظام السعودي صنعا عندما أورد نصوصا خاصة باستعمال الكمبيوتر والإنترنت في الدعوة إلى الأفكار الإرهابية .**

**- أحسن النظام السعودي صنعا عندما عاقب على صور عديدة لاستعمال الكمبيوتر والإنترنت في ارتكاب جرائم مخلة بالآداب وبالنظام العام.**

**- توسع المنظم السعودي في نظام مكافحة جرائم المعلوماتية بتجريمه لحيازة الصور والأفلام المخلة بالآداب حتى ولو كان ذلك بقصد الاستعمال الشخصي على خلاف الاتجاه العام في التشريعات المقارنة التي تعاقب على حيازة تلك المواد إذا كانت بقصد الاتجار أو الترويج.**

**وننتهي إلى توصيات من أهمها ما يلي:**

**- من الضروري إدخال نصوص خاصة لحماية النظام ولحماية المعلومات المتواجدة داخل النظام، بسبب قصور القواعد العامة في توفير الحماية المناسبة في هذا المجال. من النصوص الخاصة التي تحمي النظام: تجريم الدخول بدون وجه حق أو البقاء في النظام بدون وجه حق، وتجريم الإخلال بسير النظام، ومن النصوص الخاصة التي تحمي البيانات داخل النظام  تجريم إتلاف البيانات أو العبث بها، وتجريم انتهاك سرية المراسلات الإلكترونية، وقد تدار النظام السعودي لسنة 1428 هـ (2007م).**

**-  من الضروري توفير حماية لكلمات السر من محاولة المقتحمين التعرف عليها أو الاتجار فيها، وهو ما يصيب الأفراد والشركات التجارية بأضرار كبيرة.**

**- من الضروري تجريم إتلاف البيانات أو العبث فيها دون اشتراط أن تكون هذه البيانات على شبكة.**

**- من المناسب أن يحدد النظام السعودي المقصود بالاحتيال حتى لا تضطرب المحاكم في تفسيرها للمقصود بهذا التعبير. وفي هذا نقترح بأن يتم الاستعانة بمفهوم الاحتيال وفقا للقواعد العامة في التشريعات المقارنة والتي تعرفه بأنه استعانة الجاني بمظهر خارجي أو الاستعانة بالغير أو التصرف دون وجه حق في مال ثابت أو منقول مملوك للغير أو انتحال شخصية الغير وذلك لإيهام الغير بمشروع وهمي بغرض الاستيلاء على مال منقول مملوك للغير.**