

أمن المعلومات وآثاره على أداء المصارف التجارية  
دراسة استطلاعية على محافظة جدة (٢٠١٠)

الدكتور/ نايف صلاح الغمري  
قسم إدارة الأعمال  
كلية الاقتصاد والإدارة  
جامعة الملك عبد العزيز

## أمن المعلومات وأثارة على أداء المصارف التجارية

### دراسة استطلاعية على محافظة جدة (٢٠١٠)

#### مستخلص الدراسة:

لقد استفادت الدول المتقدمة من استخدام الآلات وحولت اقتصادياتها من الاقتصاديات الزراعية إلى الاقتصاديات الصناعية، ثم تمكنت من تطوير المعرفة عن طريق التقنية وتحويلها إلى المعرفة الرقمية. والآن تبادل المعرفة الرقمية لا يعطي أي اعتبارات للمكان والزمان. لقد أصبحت تنتقل بين شعوب العالم في كل صوب واتجاه غير معترفة بالحدود الجغرافية والسياسية.

وكما تمكنت هذه الدول المتقدمة من استخدام الصناعة كقوة للسيطرة على العالم اقتصادياً وسياسياً. استطاعت مرة أخرى من التحكم في توفير المعرفة للدول الأخرى. ولم يكن ممكناً إلا عن طريق إيمانها بالعلم والبحث العلمي.

ولقد ساهمت التقنية منذ ظهورها في تغيير الكثير من المفاهيم التي اعتاد الناس عليها. ففي الوقت الذي استطاعت فيه أن تساهم بصورة إيجابية في اختصار الوقت والمسافات بين الأمم، إلا أنها أفرزت بعض الميزات السلبية مثل صعوبة احتفاظ الفرد بخصوصياته.

وكما عرفنا منذ نشأت أظفارنا بقصص السرقة التي يتعرض لها البعض من سرقة الأموال والأشياء الثمينة، إلا أنه في عصر التقنية ظهرت أنواع جديدة من السرقات التي لا تحتاج إلى اقتحام البيوت والمصارف، وهي سرقة قرصنة الإنترنت وتتمثل في سرقة الهوية وتحويل الحسابات من رصيد إلى رصيد آخر وسرقة المعلومات الحساسة والمعلومات العسكرية.

لذا لأمن المعلومات دور كبير في حياتنا، وأصبح من أولويات اهتمامنا. وفي هذا البحث سوف نركز على تقييم العملاء لأمن المعلومات في المصارف التجارية بل واعتباره أحد أبعاد الجودة الرئيسية التي تعتمد معظم المصارف في إظهاره كأحد المزايا التنافسية التي تحاول أن تحتفظ بها.

هذا وقد اشتملت دراسة البحث على خمسة أجزاء هي:

١. الجزء الأول: تناول مشكلة البحث وأهدافه وأهميته وفروضه.
٢. الجزء الثاني: تناول الإطار النظري للبحث والدراسات السابقة.
٣. الجزء الثالث: تطرق لمنهج البحث وأدوات جمع البيانات وطرق قياسها والتحقق من صدقها والأدوات الإحصائية المستخدمة.
٤. الجزء الرابع: تناول تحليل نتائج الدراسة الميدانية واختبار صحة الفروض.
٥. الجزء الخامس: ركز على نتائج وتوصيات البحث.

The Affects of Information Security on The efficiency of  
Bank Competition Roles in Jeddah Province (2010)

## Salah Ghamri Nayef

Assistant Professor, Department of Business Administration  
King AbdulAziz University, Jeddah, Saudi Arabia

### Abstract

This study well discuss the most important security issues as well as some solutions to them. Information is one of a bank's most important assets. Protection of information assets is necessary to establish and maintain trust between the bank and its customers and protect the reputation of the bank. Timely and reliable information is necessary to process transactions and support bank and customer decisions. When information becomes known to unauthorized parties, this means banks lost availability, reliability, confidentiality, accountability and operational security. The proposed study aims at defining the information security. The study is an attempt to analyze information security problem and find means to reduce it. The information security acts as one of the most important factor which affects the bank customers and bank performance. This information security problem arises from different sources. These sources are: The customers educational and social backgrounds, which leads to increase in information security problem. The lack of bank workers training. Lack of cooperation between the manager and the

employees leads to conflict. When the role of information security is not properly defined by managers, information security problem is going to be a result. However using Internet in banking means that it has advantages and disadvantages : it can give customers good services, but it allows many bad people to access to your accounts.

However this study includes a theoretical as well as a field components. The theoretical part considers information security problem: its influence, sources, effects and the strategies adopted to remedy it. It also emphasizes on the concept of quality services. The field part is to define the relationship between the information security problem and the extent of its effect on banks performance.

After pilot testing , a questionnaire was administered to 90 managers and customers, yielding 60 sets of complete data (67 percent ). These data represented the responses of 30 managers and 30 customers. Although, sets of questionnaires distributed among the employees, banks were designed to collect the required information. In analyzing the data, the researcher used the frequencies, percentages and chi - square methods. A sixty questionnaires were received. The result of the study indicated that customers educational and social backgrounds and lack of bank workers training were the most important sources of information security problem. However, role facilities that process and maintain information were the least sources of information security problem. In the light of the result of this study, the

researcher gave recommendation to reduce the affects of sources of information security problem.

## أولاً: الإطار العام للبحث.

### المقدمة

يقع الأمن في المرتبة الثانية من سلم أولويات الحاجات الضرورية لدى علماء النفس والاجتماع ويتسع مفهوم الأمن في وقتنا الحاضر ليشمل الأمن الثقافى، والأمن الغذائى، والأمن الاقتصادى، والأمن الاجتماعى ، والأمن العسكرى، والأمن الصحى، والأمن الصناعى، والأمن البيئى، والأمن السياحى، والأمن المهنى، والأمن الوطنى، والأمن الإقليمى، والأمن الدولى، وغيرها من المجالات الأمنية التي يتطلبها الفرد والمجتمع<sup>١</sup>.

والمعلومات هي سمة العصر الذي نعيشه وشبكات المعلومات هي الخلايا العصبية التي تتولى نقل المعلومات إلى كل مكان.

وعبارة أمن المعلومات يمكن تعريفها "بأنها العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية والخارجية. والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين ولضمان أصالة وصحة الاتصالات، وأمن المعلومات هو فكرة قديمة ولكن بدأت استخداماته بشكل مكثف منذ تطور التكنولوجيا وخاصة الإنترنت لذا كان لابد من أمن المعلومات للمحافظة على سرية معظم المعلومات السرية"<sup>٢</sup>.

<sup>١</sup> آل ناجي محمد ، (١٤٢٥) ، نحو برنامج عملى لتنمية الدور الأمنى للمؤسسات التربوية ، ورقة عمل مقدمة لندوة المجتمع والأمن المنعقدة بكلية الملك فهد الأمنية بالرياض ، جامعة الملك خالد كلية التربية ، أبها، ص ١.

<sup>٢</sup> ويكيديا - الموسوعة الحرة ( أمن المعلومات ).

وقد استخدمت فكرة أمن المعلومات Information Security قبل الميلاد منذ أيام الرومان، وكانت المعلومات العسكرية تمثل أحد ركائز النصر. ومع ظهور التقنية الحديثة والتغير في اتجاهات الفكر الثقافى والمهتم بالازدهار والرخاء الاقتصادي، أصبح العالم يهتم بالمعلومات بصفة عامة والمعلومات المالية والاستثمارية بصفة خاصة، والتي لعبت وسائل الاتصال من الحاسب الآلي والإنترنت دور كبير في جاهزية وسهولة استخدامها، ومن هنا ارتبطت كلمة أمن المعلومات حديثاً بشبكة الإنترنت والحاسب الآلي. وكان موضوع أمن المعلومات يحتل جل إهتمام الباحثين والمسؤولين والشرع والأفراد العاديين على حد سواء.

و"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، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفير المعلومات ومكافحتها".<sup>1</sup>

ومع انتشار ثقافة المعلومات والمجتمع المعرفي، ظهرت أمية الحاسب الآلي Computer Illiteracy والتي تتمحور في عدم قدرة الأفراد وإن كانوا ذو مستوى علمي رفيع على التعامل مع وسائل الاتصال من شبكة الإنترنت والحاسب الآلي.

<sup>1</sup> الزهيري طلال ، الحاسوب الشخصي ومتطلبات امن المعلومات ، قسم المعلومات في الجامعة المستنصرية ص ٣

## مشكلة البحث:

يتطلب التطرق لأمن المعلومات للتعرف على:

- ❖ أمن المعلومات.
- ❖ ما هي الآثار المحتملة لإختراق أمن المعلومات والأسرار المالية الشخصية؟
- ❖ ما هي أنجح الحلول التي تتناسب والواقع الحالي لحل مشكلة أمن المعلومات؟

## أهداف البحث:

بناء على الوصف السابق للمشكلة فإنه يمكن تحديد أهداف البحث والتمثلة في التالي:

- ❖ التعرف على أمن المعلومات والتعرف على هذه الظاهرة وبيان أبعادها ، ومدى خطورتها وأضرارها.
- ❖ بيان الصور والأنماط المستحدثة لجرائم أمن المعلومات بغرض التوعية من الوقوع في حبالها وكيفية مكافحتها على الوجه الأمثل ، والتبنيه إلى أوجه القصور في مكافحة أمن المعلومات.
- ❖ الكشف عن جرائم أمن المعلومات التي أصبحت ظاهرة عالمية ووجوب تضافر الجهود الاجتماعية والثقافية والإعلامية ، وجهود الشرطة والمنظمات والمؤسسات الدولية والإقليمية.

## أهمية البحث:

تظهر أهمية البحث في أنه يتناول أهم نواحي الحياة وهي سرية المعلومات الشخصية والمالية ، ويتوافق مع التقدم السريع في التقنية ومع براعة قرصنة الإنترنت في قدراتهم على إختراق أمن المعلومات والسرية الشخصية.

ويعتبر أمن المعلومات من أنشط القطاعات المعلوماتية وأكثرها تطوراً ويحظى بنصيب كبير من البحث العلمي في الجامعات والمؤسسات لأهميته وتعدد فروعها ومجالاته. ويبرز عدد من التساؤلات مثل:

- ❖ ما هي عناصر أمن المعلومات؟.
- ❖ ما هي عمليات المعلومات الرئيسية المتصلة بأمن المعلومات؟.
- ❖ ما هي المخاطر والتهديدات ونقاط الضعف؟.
- ❖ ما هي أنواع الهجمات والاعتداءات وأساليبها التقنية؟.
- ❖ ما هي إستراتيجية أمن المعلومات وكيف يتم بناؤها؟.

#### متغيرات البحث:

هناك نوعان من المتغيرات وهما المتغير التابع ويتمثل في مستوى الأداء لدى المديرين والعملاء. والمتغير المستقل وهو أمن المعلومات.

#### فروض البحث:

يتناول البحث عدة فروض، ومنها:

- ❖ الفرض الأول: وجود اختراق لأمن المعلومات البنكية.
- وقد تضمن أسئلة الاستبيان التالية ١- ٢- ٣- ٤- ٥- ٦- ٧- ٣٢- ٤٤- ٣٣

- ❖ الفرض الثاني: تتباين عمليات اختراق أمن المعلومات بين المصارف

التجارية كلاً حسب قدراته التقنية وخبرات الموارد البشرية لديه.

- وقد تضمن أسئلة الاستبيان التالية ٨- ٩- ١٠- ١١- ١٢- ١٣- ١٤- ٤٣- ١٥

❖ الفرض الثالث: هناك علاقة بين أمن المعلومات والمستوى الثقافى

والتعليمى للمستفيدين من الخدمة.

وقد تضمن أسئلة الاستبيان التالية ١٦- ١٧- ١٨- ١٩- ٢٠- ٢١- ٢٢-

❖ الفرض الرابع: هناك علاقة بين جودة أداء وكفاءة وجاهزية المصارف

التجارية ومخرجات أمن المعلومات المتمثلة فى رضا العميل وحماية

المعلومات الشخصية والمالية.

وقد تضمن أسئلة الاستبيان التالية ٢٣- ٢٤- ٢٥- ٢٦- ٢٧- ٢٨- ٢٩- -

٣٠- ٣١- ٤٥-

❖ الفرض الخامس: هناك علاقة طردية ذو دلالة إحصائية بين تقدم التقنية

والقدرة على مكافحة سرية المعلومات.

وقد تضمن أسئلة الاستبيان التالية ٣٤- ٣٥- ٣٦-

❖ الفرض السادس: علاقة بين أمن المعلومات وتعاون بعض موظفي

المصارف فى عملية الاختراق.

وقد تضمن أسئلة الاستبيان التالية ٣٧- ٣٨-

❖ الفرض السابع: هناك علاقة بين قوة الإجراءات القانونية والقضائية

والقدرة على مكافحة سرية أمن المعلومات.

وقد تضمن أسئلة الاستبيان التالية ٣٩- ٤٠- ٤١- ٤٢-

## ثانياً: الإطار النظري والدراسات السابقة:

لقد كان تأثير شبكة الإنترنت كبير على نمط حياتنا اليومية، فقد مكنت شبكة الإنترنت الأفراد من الاستفادة من المزايا غير المحدودة التي تتميز بها هذه الشبكة، ومكنت عملاء المصارف الاستفادة من الخدمات الإلكترونية التي تقدم لهم بكل الوسائل الممكنة والمريحة للحصول على الخدمة. وفي عصر الإنترنت لا يحتاج العميل أن ينتظر أمام البنك حتى يفتح أبوابه ليسحب من رصيده، ولا يحتاج أن يستعجل الوقت لأن يقوم بعملية حسابية قبل أن يغلق البنك أبوابه، فقد جاءت الخدمات الإلكترونية غير معطيته أي اهتمام للوقت والمكان، وأصبح بإمكان العملاء إجراء العمليات الحسابية أو التجارية في أي مكان في المعمورة وفي أي وقت وبسرعة فاقت كل خيال بشري، وأصبح ارتباط الجوال مع الإنترنت من أجمل مظاهر هذا العصر الرقمي وأصبح من الصعوبة بمكان ومن حكم المستحيل الفصل بين الإنسان والحاسب الآلي والإنترنت في وقتنا الحاضر.

إلا أن أجهزة الحاسب الآلي قد تحوي معلومات حساسة ومهمة للفرد والمنظمة، مما قد نتج عنه أساليب وممارسات جديدة لضمان البيانات والمعلومات على هذه الأجهزة، وقد ارتبط مع هذه الأجهزة ظهور بروتوكولات جديدة ذات مواصفات عالية الدقة سهلت تخاطب هذه الأجهزة مع بعضها البعض، وهذه البروتوكولات هي البلوتوث، الواي فاي، والإنترنت، وترتب على ذلك ثغرات أمنية سمحت باختراق تلك الأجهزة بعلم أو بدون علم مستخدميها مما وجب نشر وعي ثقافة أمن المعلومات، لأن هذه المخاطر لن تتلاشى، والشركات الناجحة يجب أن تتبنى استراتيجيات لتقليل تلك المخاطر مع تقديم حلول فعالة لعملائها. وفي

الواقع فإن أمن المعلومات يمكن أن يستخدم كإستراتيجية للمنافسة بين المصارف، خصوصاً في ظل اتساع رقعة استخدام شبكة الإنترنت.

"وتشير إحصاءات تقرير مؤسسة التكنولوجيا الألمانية المتطورة (Advanced German Technology - AGT) إلى أن الاحتياطي المخصص لدول المنطقة العربية للإنفاق على أمن المعلومات حتى عام ٢٠٠٤ لا يتجاوز ٢٠٠ مليون دولار في حين إن المطلوب توفيره هو ٥ مليارات دولار، وأشارت التقديرات انه يتعين على القطاع الخاص التعاون مع القطاع الحكومي في مجال المصارف بشكل خاص، وضرورة أن تتبنى إستراتيجية مؤثرة لأمن المعلومات وانتقد التقرير تساهل المؤسسات والمصارف في الحفاظ على سرية وأمن المعلومات وأرجع التقرير القصور إلى عدم وجود هيئة أو مؤسسة تقوم بتنظيم أمن المعلومات. وتمثل دول الخليج العربي النصيب الأكبر من إجمالي تطبيقات البيئية الرقمية في الوطن العربي. يوضح الجدول التالي: مؤشر استخدام تكنولوجيا المعلومات في دول مجلس التعاون ومصر".<sup>١</sup>

الدولة	عدد السكان	عدد الحواسيب	عدد مستخدمي الإنترنت	مؤشر استخدام تكنولوجيا المعلومات والاتصالات
الإمارات	٣.٧٠٠.٠٠٠	٥٩٠.٠٠٠	١.١٠٠.٠٠٠	١.٤٣
البحرين	٧٢٨.٠٠٠	١٠٨.٠٠٠	١٨٠.٠٠٠	١.١٨
الكويت	٢.٤١٨.٠٠٠	٣٠٠.٠٠٠	٣٢٠.٠٠٠	١.٠٤
قطر	٨٠٥.٠٠٠	١٠٨.٠٠٠	٧٥.٠٠٠	٠.٨

<sup>١</sup> مكاوي محمد، البيئة الرقمية بين سلبيات الواقع وآمال المستقبل *Cybrarians Journal*، سبتمبر (2004).

٠.٥٣	١.٩٢٠.٠٠٠	١.٨٠٠.٠٠٠	٢٣.٨٩٨.٠٠٠	السعودية
٠.٣٦	١٦٥.٠٠٠	٩٧.٠٠٠	٢.٧٦٠.٠٠٠	عمان
٠.٢٢	٢.٠٠٠.٠٠٠	١.١٣٠.٠٠٠	٧١.٣٠٠.٠٠٠	مصر
٤.٨١	٥.٧٦٠.٠٠٠	٤.١٣٣.٠٠٠	١٠٥.٦٠٩.٠٠٠	المجموع

وتركز المملكة العربية السعودية على الحق المعلوماتي للمواطن والمقيم على حد سواء ، والحفاظ على سرية المعلومات الشخصية والمالية وأيضاً على الحقوق الفكرية.

وهناك أحكام قانونية تضمن خصوصية الأفراد وأحكام تتطرق للاستخدام السيئ للإنترنت مثل الشتم وتغيير الحقائق الشخصية والاختراق وانتحال الشخصية.

### مكونات أمن المعلومات :

- ❖ سرية المعلومات
- ❖ سلامة المعلومات
- ❖ ضمان جاهزية المعلومات .

أولاً: سرية المعلومات : من المشاكل التي تحصل لمستخدمي الإنترنت هي عملية إحتراف البيانات والمعلومات والإطلاع عليها من أفراد دخلاء وغير مصرح لهم. ومن ضمن عمليات الإختراق هذه، الإطلاع على المعلومات العسكرية للدولة ، المعلومات المالية للمصارف والأفراد ، والمعلومات الشخصية.

ثانياً : سلامة المعلومات : عمليات تغيير المعلومات كثيراً ما تحصل في المصارف والأسواق المالية . فقد تبدأ بعملية إختراق سرية معلومات شخص ما في مصرف

ما ومعرفة رصيده ، ثم يتم بعد ذلك المرحلة الثانية وهي التغيير في معلومات العميل مثل تغيير قيمة المبلغ المحول من رصيد إلى رصيد آخر، فمثلاً في حالة تحويل ألف دولار من حساب شخص إلى آخر ، يتم تحويل عشرة آلاف دولار .

ثالثاً : تعطيل المعلومات : فقد يقوم بعض مجرمي الحاسب بتعطيل الحاسب أو تباطؤ استخداماته وبذلك يؤدي إلى تعطيل عمل المنظمة ككل.

وهناك بعض الأفراد الذين لهم الصلة باختراق المعلومات .

وفي أغلب الأحيان يتم اختراق المعلومات بطريقتين:

أولاً: المخترق الداخلي: تتم عن طريق الأفراد الذين يعملون في المنظمة (موظفي المصرف مثلاً) وهؤلاء أشد قدرة على اختراق سرية معلومات المنظمة من الأفراد الخارجين عن المنظمة، ودائماً ما تقوم الشركات كالمصارف بحل المشكلة بكل سرية حتى لا يؤثر ذلك على سمعة البنك وفقدان الثقة من قبل العملاء بالمصرف.

ويرجع السبب في اختراق المعلومات إلى عدة عوامل يمكن إختصارها في التالي :  
أ - استخدام المعلومات المتوفرة للمكاسب المادية ، مثل المعلومات عن شخصيات هامة أو معلومات عسكرية أو معلومات عن بنود العقود والمناقصات.

ب - قد يقوم بعض الأفراد بالشعور بعدم الرضا عن المنظمة التي يعمل بها ، فيقوم باختراق المعلومات وتسريبها إلى الآخرين وغالباً ما يكون ذلك بعد إنهاء خدمة هؤلاء الأفراد ، ويسمى هؤلاء بإسم (أطفال البرامج الجاهزة).  
ويشعر هؤلاء الأفراد بالرضا النفسي نتيجة تحقيق أضرار مادية لهذه الشركة أو الشعور بالفخر لقدرته على اختراق سرية المعلومات في المنظمة.

هذا وقد يستطيع المخترق الداخلي أن يقوم بتوفير نقاط العبور والممرات الإلكترونية للغير للإختراق والإطلاع على أسرار المنظمة لما لديه من تسهيلات أكثر من المخترق الخارجي إضافة إلى داريته بأنظمة الشركة وخبائها وإمكانية الوصول للمعلومات الحساسة أكثر من المخترق الخارجي.

ثانياً: المخترق الخارجي: وهم الأفراد الذين يخترقوا أمن المعلومات ويطلعوا على أسرار المنظمة ، والهدف من القيام بهذه العمليات هو:

١. سرقة المعلومات القيمة مثل الأسرار المالية والشخصية.
٢. التجسس على الآخرين، وقد انتشرت عمليات التجسس خصوصاً السنوات الأخيرة ليس فقط بين الدول، بل بين شركات الأموال والشركات الصناعية. مثل التجسس على الاختراعات والأبحاث العلمية التي تقوم بها هذه الشركات ، كعرفة موديل سيارة جديدة قبل نزولها إلى الأسواق بفترة زمنية ، أو التجسس على بيانات كبار الشخصيات.

ونظراً لأن " محاولة اختراق الشبكات من خارجها أمر ليس بالسهل، لذا يتم الاعتماد على العنصر البشري كمحاولة إدخال شخص لمبنى المؤسسة، أو استقطاب شخص من موظفيها، وهو الأمر الذي أثبت جدواه في العديد من الحالات، لدرجة أصبحت معها الاختراقات الداخلية أكثر ضرراً من الخارجية، لأنها تشكل كما يقول الخبراء ٨٠ في المائة من الاختراقات التي تتم في العالم. وبخاصة وأن الإهمال البشري يلعب دوراً في جعل ذلك ممكناً. فعلى سبيل المثال هناك نموذج كمدير البنك الذي يغادر مكتبه بعد يوم عمل طويل، تاركاً وراءه أوراقه وبياناته ملقاة ومكشوفة على مكتبه، فتدخل عاملة التنظيف، أو من يتستر بشخصيتها، لتأخذ أو تصور نسخاً عن هذه الوثائق، وربما تستطيع أن

تجد كلمة السر الخاصة به لدخول الكومبيوتر، مكتوبة على ورقة ملصقة على شاشة الجهاز، وهو ما يعتبر صيدا لا يقدر بثمن<sup>١</sup>.

٣. التخريب لتعطيل مهام أنظمة الحاسوب عن طريق تعطيل شبكة الاتصالات الداخلية وهي هنا الأهم لأنها مركز المعلومات السرية في الشبكة الداخلية التي تخص المنظمة وهي تحتوي على معلومات جوهرية.

وقد تستخدم بعض المنظمات الكبيرة الحجم مثل الجامعات والوزارات التي تمتاز بحساسية معلوماتها (مثل وزارة الدفاع والمالية والبنوك المركزية للدول)، نوعان من الشبكات وهي الشبكة الداخلية والشبكة الخارجية. أما الشبكة الداخلية فهي التي تتمركز بها المعلومات الخاصة بالمنظمة والتي تمتاز بالسرية العالية، أما الشبكة الخارجية فهي تحتوي على معلومات إعلانية من الدرجة الأولى ولها علاقة بالإنترنت وغالباً ما تكون هاتان الشبكتان مفصولتان عن البعض. والسبب يرجع إلى أن كثير من المنظمات ترى أن المخترقين لأنظمة الحاسب وأمن المعلومات يتم عن طريق الإنترنت، ثم أن كثير من الفيروسات تنقل عن طريق الإنترنت، وهنا يستطيع المخترق الداخلي عمل جسر بين الشبكة الداخلية والخارجية أو في بعض الأحيان العمل على توصيل الفاصل بين الشبكتين حتى يؤدي إلى تعطيل الشبكة من طريق الفيروسات أو تمكين المخترق الخارجي للوصول إلى الشبكة الداخلية.

<sup>١</sup> شبيب أنس، حماية المعلومات صارت مسألة حماية للاقتصاد الوطني، جريدة الشرق الأوسط، العدد ٩٢٩٢ تاريخ ٢١ ربيع الأول، سنة ١٤٢٥.

## أنواع الإقتحام :

### ١. إنتحال الشخصية.

انتحال الشخصية يتم عن طريق معرفة الرقم السري لبعض مستخدمي الإنترنت و "يمكن أن يحدث خطر انتحال الشخصية عن طريق قيام المهاجم بسرقة مفتاح التشفير السري أو إقتناص كلمة السر خلال مرورها بالشبكة وإعادة إرسالها في وقت لاحق"<sup>١</sup>

وقد "يقوم المهاجم بتزويد معلومات توجيه الرسالة بحيث يغير من مسار الرسائل الصادرة من مركز البنك الرئيسي إلى أحد فروعها بحيث تمر هذه الرسائل على طريق آخر يمر بمنطقة نفوذ المهاجم وفي المسار الجديد يمكن تسجيل الرسائل".<sup>٢</sup>

وقد تبنت كثير من المصارف فكرة استخدام الفأرة (الماوس) في إدخال الأرقام السرية حتى لا يتمكن المهاجم من اقتناص الرقم السري. وأصبح التجسس على شبكات المعلومات والإنترنت بهدف الحصول على رقم بطاقة الإئتمان من المشاكل التي غالباً ما تكلف المصارف وشركات التأمين أموال باهظة.

### ٢. الفيروسات:

قد يستخدم المهاجم نوعاً معيناً من الفيروسات بهدف السيطرة على بعض المعلومات الهامة. وقد سميت بالفيروسات لتشابه صفاتها مع الفيروسات التي تصيب الإنسان والحيوان على حدٍ سواء. من ضمن هذه الصفات ، صفة

<sup>١</sup> داود حسن، (١٤٢٥)، أمن شبكات المعلومات، معهد الإدارة العامة، الرياض، ص١٠٢.

<sup>٢</sup> داود حسن، (١٤٢٥)، أمن شبكات المعلومات، مرجع سابق، ص ١٠٢.

الإنتشار السريع مثل الأمراض الوبائية التي تنتشر بين الأشخاص نتيجة انتقال الفيروس من شخص لآخر بالعدوى، وتطفله على الجسم البشري وإلحاق الضرر به لكونه جسم غريباً على جسم الإنسان، بالإضافة إلى الأضرار الناتجة قبل وبعد العلاج، والفيروسات لها صفتين رئيسيتين:

الصفة الأولى: وهي صفة التستر والسيطرة على البرنامج المصاب، ففي حالة تشغيل البرنامج المصاب بالفيروسات، تبدأ الفيروسات في العمل سويّاً.

الصفة الثانية: "انتقالها يشبه طريقة انتقال الفيروسات البيولوجية حيث تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكرة (رام)، وتصيب أي ملف يشغل في أثناء وجودها بالذاكرة مما يزيد عدد الملفات المصابة، كلما تأخر وقت اكتشاف الفيروس كلما كان تدمير الفيروس أقوى".<sup>١</sup>

والفيروسات هي أي برامج أو مجموعات من التعليمات التي تلحق ضرراً بنظام المعلومات أو بالبيانات على أن تكون لديها القدرة على التضاعف والإنتشار.<sup>٢</sup>

<sup>١</sup> الزهيري طلال، الحاسوب الشخصي ومتطلبات أمن المعلومات، الجامعة المستنصرية، العراق، ص ٥.

<sup>٢</sup> داود حسن، أمن شبكات المعلومات، ص ١٦٦، مرجع سابق.

## مراحل نظام أمن المعلومات:

### أولاً - مرحلة التقييم:

يعتبر تقييم مخاطر أمن المعلومات من حيث معرفة البيانات والمعلومات المهمة والحساسية من أهم المراحل في نظام أمن المعلومات، ويتطلب التقييم ليس فقط حساسية المعلومات بل أيضاً إيجاد الأفراد المتخصصين والمتدربين والذين لديهم القدرات والمعرفة للتقييم والحماية المستمرة وتطوير سبل حمايتها.

### ثانياً - مرحلة التصميم:

إذا افترضنا أن الأمن سلسلة، فإن السلسلة تقاس بأضعف حلقة من حلقاتها. لذا فإن استخدام أحدث الحواجز الشبكية (أو حتى أنظمة كشف الاختراقات) لا يضمن الأمن التام للمنشأة. ولكن يجب اعتماد هيكلية أمنية صلبة عند تصميم البنية الأساسية لأمن المعلومات. إن اتخاذ أساليب دفاعية عميقة هي إستراتيجية فعّالة لتحقيق الضمان في هذا العصر الذي يعتمد اعتماداً كبيراً على البيئات الشبكية<sup>1</sup>.

### ثالثاً - مرحلة التنفيذ:

على المنظمة أن توفر هياكل أمنية تتناسب مع ضوابط التقنية التي تختارها، ومن هذه الضوابط، الحاجز الشبكي، ونظام كشف الاختراقات. وللضمان الذي تحصل عليه المنظمة دور كبير في التخفيف من المخاطر ويتمثل ذلك في المشورة التي تقدمها الشركة الموردة بحكم دورها المحايد للتعرف على درجة

<sup>1</sup> حسيني صلاح، (٢٠٠٨)، أمن المعلومات لأنظمة المعلومات، بحث ماجستير غير منشور، بغداد،

لرابط: <http://www.iraqstudent.net/detail.php?recordID=694>.

الأمان في البنية الأساسية، حيث يكون لديها الخبرات لتقييم البرامج الأمنية والتجهيزات ومطابقة البنية التحتية للنظام ككل.

#### رابعاً - مرحلة المراقبة:

مراقبة نظام المعلومات عملية معقدة ومكلفة ولكنها ضرورية في ظل الإبداع الذي يمتاز به مخترقي الأنظمة، لذلك عملية حماية ومراقبة النظام لن تكون آمنة بالكامل خصوصاً التي لها علاقة بالنواحي المالية. لذلك على المنظمة أن توظف أفضل الأفراد الذين يستطيعون مراقبة أنظمة المعلومات وتجهيزاتها 24 ساعة يومياً، 365 يوم سنوياً. إن وضع اللوائح التنظيمية ووضوحها ومراقبة الأفراد على تنفيذها يساعد كثيراً في الحد من مخاطر أمن المعلومات، ويلعب تثقيف العاملين في المنظمة دور فعال في عملية أمن المعلومات. إذا كانت الحواجز الشبكية لها دور كبير في الحد من مخاطر أمن المعلومات فإن الحواجز البشرية لا تقل أهمية عن الحواجز الشبكية.

#### العناصر الأساسية الواجب توفرها لحماية المعلومات :

- ❖ السرية : وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها أشخاص غير مخولين بذلك .
- ❖ سلامة المحتوى: التأكد من إن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به في أية مرحلة من مراحل المعالجة.
- ❖ استمرارية توفر المعلومات: التأكد من استمرارية جاهزية النظام واستمرارية القدرة على التعامل مع البيانات و المعلومات.

❖ عدم إنكار التصرف المرتبط بالمعلومات ممن قام به: ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار انه هو الذي قام بهذا التصرف.<sup>١</sup>

### أهم الوسائل للحد من الجريمة الرقمية أو المعلوماتية :

لقد أطلق الباحثين المتخصصين في علم نظم المعلومات عدة مصطلحات على الجرائم التي تتم عن طريق استخدام التقنية الحديثة. فمنهم من أطلق عليها الاختلاس المعلوماتي والآخر أطلق عليها الاحتيال المعلوماتي والبعض الآخر الغش المعلوماتي وكلها ارتبطت بتطويع التقنية الحديثة في العمليات غير القانونية وعمليات الإجرام والسرقة.

"والمعلوماتية هي كلمة مكونة من مقطعين، المقطع الأول Information والمقطع الثاني Automatique ويرجع الفضل في اقتراح مصطلح المعلوماتية إلى Drefus حيث استخدمه عام ١٩٦٢ لتمييز المعالجة الآلية للمعلومات وثبته بعد الأكاديمية الفرنسية في ابريل ١٩٦٦ ومنحته التعريف الآتي - علم المعالجة المنطقية للمعلومات"<sup>٢</sup>

ويرى Tredmann أن " الجريمة المعلوماتية تشمل أي جريمة مرتبطة باستخدام المعالجة الآلية للمعلومات".<sup>٣</sup>

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام المخالفة (الجريمة ) في كل حالة يتم فيها " تغيير معطيات أو بيانات أو برامج الحاسوب

<sup>١</sup> مكايي محمد، (٢٠٠٩) البيئة الرقمية بين سلبيات الواقع وآمال المستقبل، دار الكتب والوثائق القومية، ص ١.

<sup>٢</sup> الشوا سامي، (١٩٩٤) ثورة المعلومات وانعكاساتها على قانون العقوبات ، القاهرة ، دار النهضة العربية، ص ٤.

<sup>٣</sup> مومني نهلاء، (٢٠٠٨)، الجرائم المعلوماتية، عمان، دار الثقافة، ص ٤٨.

أو محوها أو كتابتها أو تدخل آخر في مجال إنجاز البيانات أو معالجتها، وتبعاً لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو يقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر".<sup>1</sup>

وقد حظي مبدأ الحد من الجرائم الرقمية وأمن المعلومات اهتمام أغلب دول العالم خصوصاً الدول الصناعية، والتي تمتاز بتقدم تقني كبير بحيث يلاحق قضائياً الأفراد الذين يقومون باستخدام الحاسب للحصول على مبالغ مالية بأي الطرق المستخدمة مثل تحويل الأرصدة أو بيع معلومات شخصية أو معلومات حكومية أو بتعديل في برنامج الحاسب والتي قد تسبب أخطار للغير.

هذا ولقد أهتم ديننا السمح بحقوق الأفراد وخصوصياتهم وذكر في القرآن الشريف في الآية (ولا تأكلوا أموالكم بينكم بالباطل) وفي الحديث الشريف، (المسلم على المسلم حرام دمه وماله وعرضه) ويقصد هنا أن استخدام أي وسيلة من الوسائل سواء كانت وسيلة تقليدية مثل السرقة أو السطو أو استخدام وسائل التقنية الحديثة مثل الإنترنت في تحويل المبالغ من رصيد إلى رصيد آخر يعتبر سرقة.

وأدى الاعتماد الكبير على شبكة الإنترنت، إلى زيادة حوادث أمن المعلومات مما حدا بالحكومات في دول مجلس الخليج العربي إلى سن التشريعات القضائية لحماية مستخدمي هذه الشبكة، وقد ركزت تلك القوانين على عدة محاور منها على سبيل المثال: تشريعات تخص معلومات العملاء ومستخدمي شبكات الإنترنت المصرفية، وتشريعات تتعلق بالأسرار الطبية، وقوانين سرية

<sup>1</sup> السعيد كامل، (١٩٩٣)، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، دار النهضة، ص ٣٢٤.

المعلومات الشخصية الموجودة في الدوائر الحكومية وحمايتها من الانتشار، والقوانين المرتبطة بالأمور الائتمانية في المصارف وبيوت الأموال. ونظراً لسهولة الدخول إلى شبكة الإنترنت والتعامل عن طريقها في كافة أنحاء الكرة الأرضية، وعليه فليس من المهم تطبيق القوانين والتشريعات ذات العلاقة بأمن المعلومات في البلد الموجودة به الشركات، بل يجب أن تطبق كافة التشريعات والقوانين الملزمة في البلدان التي يوجد بها عملاء لتلك الشركات والمنظمات وضرورة سن التشريعات الدولية المتكاملة.

"وتكمن صعوبة التعاون الدولي حول الجريمة المعلوماتية في أنه لا يوجد مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة. بالإضافة إلى نقص الخبرات لدى الشرطة والقضاء في هذه المجال لتمحيص عناصر الجريمة المعلوماتية إن وجدت وجمع الأدلة عنها للإدانة فيها يشكل لائق".<sup>١</sup>

ومن وسائل الحد من الجرائم الرقمية الآتي:

١. تقليص الصلاحيات لأدنى مستوى بحث يكون تركيز الصلاحيات في المستويات العليا مع إعطاء صلاحيات القراءة للمستخدمين في المستويات المتوسطة والإشرافية واستمرار المراقبة عليهم.

٢. تكثيف التعاون الدولي في جميع أنحاء العالم للحد من جرائم أمن المعلومات.

٣. الاعتماد على وسائل تقنية متقدمة مثل استخدام البيانات الحيوية Biometrics مثل بصمة الإصبع والعين والوجه. لما تمتاز به من السرعة في

<sup>١</sup> الهيتي محمد، (٢٠٠٦)، جرائم الحاسوب، عمان، دار المناهج.

إتمام العمليات الخاصة بالتحقق من صحة الهوية، وربطها بقاعدة بيانات مركزية ودولية مثل المطارات ووزارات الداخلية.

٤. سن قوانين تعاقب مثل هذه الجرائم سواء ارتكبت على أراضي الدول صاحب الحق أو أراضي أجنبية .

٥. رفع مستوى قدرات القضاة والاستعانة باستشاريين ومدققين من الخارج.

٦. عمل عمليات مراجعة وتدقيق دوري لإجراءات الحماية والأمان.

٧. استخدام الجدران النارية مع كلمات السر وبصمات الأصبع والعين.

٨. تحسين مستوى الصيانة والتركيبيات.

٩. التركيز على اتفاقية أمن المعلومات بخصوص جرائم المعلوماتية مثل:

❖ الاحتيال والتزوير.

❖ الاستغلال الجنسي للأطفال واستعمالهم في المواد الإباحية.

❖ التعدي على حقوق المؤلفين.

### ❖ الاختراقات الشخصية والمالية. hAh

#### الدراسات السابقة:

نظراً لأهمية موضوع أمن المعلومات على كفاءة المصارف ونتيجة للتكاليف الباهظة الناتجة عن الأضرار التي تسببها الاختراقات مثل الأضرار المالية والنفسية للعملاء، فقد تزايد الإهتمام بالتعرف على أهم مصادر الاختراق وعمل الاستراتيجيات الناجحة لمكافحتها.

وأظهرت بعض الدراسات أن هناك علاقة بين أمن المعلومات وخلفيات الموظف والعمل الاجتماعي والمالية والثقافية وتوصلت هذه الدراسات إلى أن بيئة العمل

المادية، والنمو الوظيفي، والمسؤولية، والعلاقات الإيجابية وفرق العمل المتعاونة، والالتزام بالأنظمة، وكفاءة الاتصال من أكثر العوامل المؤثرة على أمن المعلومات.

وفي ورقة عمل باسم " نحو برنامج عملي لتنمية الدور الأمني للمؤسسات التربوية" للدكتور محمد ناجي مقدمة لندوة المجتمع والأمن المنعقدة بكلية الملك فهد الأمنية بالرياض تبرز دور الجامعة ومراكز البحث العلمي ومسئوليتها في تطوير الدراسات الخاصة بالنواحي الأمنية، وفي إعداد الدراسات والمشاريع البحثية بهذا المجال والتركيز على الأمن الفكري للأجيال الذين هم ركائز الأمن لأي مجتمع.

وتتضمن الورقة المواضيع التالية: -

أولاً: - مقومات الأمن والأمان في المملكة العربية السعودية ومن ضمنها أمن المعلومات.

ثانياً: - مسؤولية الأمن الوطني.

ثالثاً: - رسالة الجامعة في توظيف المعرفة والبحث العلمي في مجال الأمن الوطني وأمن المعلومات.

رابعاً: - دور مراكز البحوث ومسئوليتها في إجراء الدراسات الأمنية.

خامساً: - دور أستاذ الجامعة<sup>1</sup>.

وقد ركزت الورقة على الوعي وثقافة الأمن الفكري كركيزة مهمة في مكافحة أمن المعلومات.

<sup>1</sup> ناجي محمد، (١٤٢٥)، نحو برنامج عملي لتنمية الدور الأمني للمؤسسات التربوية، ورقة عمل مقدمة لندوة المجتمع والأمن، كلية الملك فهد الأمنية، الرياض.

ومن ما سبق يلاحظ أن الدراسة أهتمت بدور الثقافة العامة ككل في محاربة الجريمة، ومنها أمن المعلومات. حيث أن ثقافة الأفراد مثل الوعي والحيطة والحذر لها دور كبير في مكافحة جرائم أمن المعلومات.

وفي دراسة للسيد صلاح هادي الحسيني بعنوان "أمن المعلومات لأنظمة المعلومات" وضح فيها أهمية أمن المعلومات وأنه عنصر مهم لا يقل أهميته عن باقي عناصر العملية الإنتاجية من رأس المال والأفراد. وأن نظام المعلومات هو النظام المسئول عن جمع البيانات وتحليلها وحفظها وإخراجها على شكل معلومات ومن الأنظمة الرئيسية والدائمة لعملية اتخاذ القرار من هذا برزت أهميتها وأهمية وضع أنظمة وبرامج أمنية لحمايتها.<sup>1</sup>

وقد ركزت الدراسة على الاهتمام بأدوات الحماية ووسائل التقنيات الحديثة والبرمجيات المتطورة مثل كاميرات التصوير والشفرة السرية والبطاقات الممغنطة وبصمات العين واليدين وما إلى ذلك من أجهزة الحماية لحماية المعلومات من المخترقين والمستغلين، وأكدت الدراسة أيضاً على توفير التجهيزات والكوادر المتخصصة للحفاظ على أمن المعلومات واستمرار فاعليته.

وفي بحث مقدم للدكتور عمر نصيف "نظم المعلومات الإدارية ودورها في تحسين جودة الخدمات المصرفية" ذكر فيه أبعاد جودة الخدمات كمحور أساسي من محاور تحسين جودة الخدمات وقد حدد عشرة معايير لتقييم جودة الخدمات ( مستخدماً نموذج J. Rayport, F. Sviokla and )<sup>2</sup> والمعروضة في الجدول التالي.

<sup>1</sup> حسيني صلاح، (٢٠٠٨)، أمن المعلومات لأنظمة المعلومات، بحث ماجستير غير منشور، بغداد.

<sup>2</sup> Rayport, J. F., and Sviokla, J. J., *Managing in the Marketplace*, Harvard Business Review, November-December 1994, pp 141-150.

## جدول أبعاد قياس جودة الخدمات

التعريف	البعد
كون الشيء جدير بالثقة والاعتماد (إمكانية التصديق)، أمانة واستقامة المزود.	المصداقية
الخلو من الخطر الناجم من استخدام الخدمات الالكترونية المصرفية.	الأمن
إمكانية الوصول للخدمة، وسهولة الاتصال بها.	سهولة الوصول للخدمة
الاستماع إلى الزبائن، والمحافظة على إخبارهم باللغة التي يستطيعون فهمها.	الاتصالات
وضع الجهود لمعرفة الزبائن والتعرف الدقيق على احتياجاتهم.	فهم ومعرفة الزبائن
إظهار التسهيلات المادية، المعدات، الأشخاص، ووسائل الاتصالات ... الخ.	الملموسية
القدرة على إنجاز الوعود للخدمة باعتمادية وعلى نحو دقيق وصحيح.	الاعتمادية
استجابة الإدارة لمساعدة الزبائن وتزويدهم فوراً بالخدمة.	الاستجابة
امتلاك المهارات والمعرفة المطلوبة.	الكفاءة
لطف (كياسة)، الاحترام، مراعاة المشاعر، والصدافة لأشخاص الاتصال، والودية.	الدمائة (الكياسة)

وقد تم دمج هذه الأبعاد العشرة في خمسة أبعاد هي: الاعتمادية، الاستجابة،

الثقة، التعاطف، والملموسية المادية.<sup>1</sup>

ولإيضاح مدى فهم العميل لهذه الأبعاد الخمسة سوف نقوم بتوضيح هذه الأبعاد:

<sup>1</sup> العفشيات تيسير، (٢٠٠١)، أثر الجودة ورضا الزبون في تحديد الاستراتيجيات التسويقية للخدمة المصرفية، أطروحة دكتوراه، كلية الإدارة والإقتصاد، جامعة الموصل، العراق، ص ٨٠.

- **الاعتمادية:** وتعرف الاعتمادية بكونها القدرة على تقديم وعود الخدمة بشكل موثوق (التسليم حسب الموعد)، والقدرة على إنجاز الخدمة المطلوبة بدقة وثبات أي ثقة يعتمد عليها.
- **الاستجابة:** هي إدراك موظف المصرف ووعيه بتقديم الخدمة والتعاون مع العميل لمعرفة طلبات وشكاوي ومشاكل العملاء ثم القدرة على تقديم الخدمات، من معرفة الأرصدة والحسابات، من دون أي إنتظار وبسرعة، وبطريقة مستمرة عند الطلب، والتعرف السريع على مشاكلهم واحتياجاتهم.
- **التوكيد والثقة:** وهو قدرة المصرف وموظفيه على خلق جو من ثقة العملاء وكسب هذه الثقة بينهم، وهو بعد مهم جداً في الأعمال المصرفية حيث تتطلب بعض الأمور إستشارة موظفي المصرف في العمليات التي تتضمن بعض المخاطر العالية مثل الإستثمارات المالية والعينية ودور المصرف للتأمين على مخاطر الإستثمار وكسب ثقة العملاء في المصرف تتم نتيجة الخبرات السابقة مع العميل أو العملاء الآخرين.
- **التقمص التعاطفي:** التعامل مع العملاء بشكل شخصي وفردى وأن العميل هو شخص فريد له معاملة خاصة وتفهم سلوكياته والعناية به. ولكن السؤال هنا هل تتم هذه الخدمات في التعاملات الدولية بين المصارف العالمية في أعمال الإستثمارات وتحويل الأرصدة حيث تكون أغلب التعاملات إلكترونية. وهل يتنازل الإنسان عن بعض رغباته الاجتماعية لحصوله على السرعة في تقديم هذه الخدمات.
- **الملموسية المادية:** ومنها المظهر الخارجي للمبنى والتقنيات الحديثة، ومظهر الأشخاص. وتركز المصارف على الملموسية المادية لتحسين صورتها في مخيلة

العملاء مثل شكل المبنى الخارجي والداخلي والتقنيات المتطورة التي تسخرها للعملاء لتعطي تخيلاً للعملاء بأن المصرف يتميز بخدمات تفوق مستوى المصارف الأخرى وتستخدم في ترويجها لهذه الخدمات الإلكترونية<sup>1</sup>. إلا أن البحث ركز على جودة الخدمات ككل والتي يدخل من ضمنها أمن المعلومات الخاصة بالعملاء ، وربط بين محاور الجودة والمزيج التسويقي واستخدام نظم المعلومات في تحقيق أداء فعال للمصارف. عليه فقد أظهرت الدراسات السابقة أن أمن المعلومات أصبح يمثل تحد ويتصف بالتعقيد وصعوبة التحكم فيه في المنظمات الحكومية ومنظمات الأعمال على حدٍ سواء.

#### • التعليق على الدراسات السابقة:

من خلال العرض السابق للدراسات البحثية في مجال أمن المعلومات يتضح أن هناك عدداً من الدراسات التي تناولت هذا الموضوع. وركزت بعض الدراسات على الخلفيات الاجتماعية والتعليمية ودورها في مكافحة اختراقات أمن المعلومات، بينما اهتمت دراسات أخرى على دور المصارف التجارية في مكافحة هذه الظاهرة من حيث إمكانياتها الإدارية والتقنية، كما ركزت دراسات بحثية أخرى على النظرة القانونية لمكافحة أمن المعلومات. وفي هذه الدراسة القائمة فإن التركيز سوف يتم على دراسة سلبيات اختراقات أمن المعلومات ودور المصارف في مكافحتها وتطبيق الاستراتيجيات المستقبلية اللازمة لذلك. ثم معرفة التهديدات التي تواجه الصناعة المصرفية الإلكترونية،

<sup>1</sup> نصيف عمر (٢٠٠٩) ، نظم المعلومات الإدارية ودورها في تحسين جودة الخدمات المصرفية ، مجلة جامعة الأندلس ، صنعاء اليمن.

وعمليات التخريب التي يقوم بها قراصنة الإنترنت (الهاكرز)، الذين يحاولون التسلل إلى المعلومات الخاصة بالحسابات المصرفية والبيانات الاستثمارية السرية، أو يسعون إلى تنفيذ عمليات تحويل غير قانونية لأموال العملاء، والتي تؤدي إلى المسؤولية القانونية للمصارف نتيجة للخسائر المالية التي تلحق بالعملاء، وفقدان ثقة العملاء في هذه المصارف.

## ثالثاً: منهج البحث:

### مجتمع وعينة البحث:

ضم مجتمع الدراسة موظفي البنوك الذين لهم علاقة بأمن المعلومات، وقد أتيحت فرصة متساوية نسبياً لكل فرد في مجتمع الدراسة للظهور في العينة من خلال عينة اختيرت بطريقة عشوائية بلغ عدد أفرادها (عدد الاستثمارات الموزعة) تسعون (٩٠) استمارة وتم توزيع الاستبيان في محافظة جدة، بحيث يكون المستهدفين موظفي البنوك والعملاء للتعرف على دور البنوك في مكافحة اختراقات أمن المعلومات والآثار السلبية المترتبة على ذلك.

وقد استغرقت عملية التوزيع ثلاثين يوماً وكانت مواعيد التوزيع في أوقات مختلفة حسب رغبة موظفي البنك والعملاء، تم استرجاع اثنان وسبعون (٧٢) استبانته متكاملة.

لتحليل بيانات الدراسة تحليلاً عملياً يحقق أهداف البحث ويستخلص أفضل النتائج، تم إدخال بيانات الدراسة في برنامج التحليل الإحصائي بالبرمجة الإحصائية للعلوم الاجتماعية (SPSS).

صدق الأداة وثباتها: وتعني إن مقياس الدراسة يمكن إن يحقق الهدف وقياس الأبعاد المطلوبة فيما لو تم استخدامه في دراسة أخرى ذات معطيات متشابهة، وقد تم استخدام عدة اختبارات للتأكد من ذلك وهي كالتالي:

❖ الصدق الظاهري: FACE VALIDITY التأكد من إن مكونات

الاستمارة يمكن أن تعبر عن هدفها وتوفر البيانات المطلوبة بدقة ولتحقيق ذلك تم

عرض الاستبيان على مجموعة من الخبراء في التخصص وكذلك توزيع الاستبيان على عينة مبدئية PILOT STUDY من مجتمع الدراسة بهدف قياس مستوى فهم العبارات والمصطلحات الواردة فيها ومدى وضوحها.

❖ صدق المحتوى: CONTENT VALIDIY ويعني درجة تعبير فقرات

الاستبيان عن أبعاد الدراسة المختلفة حيث تم التركيز على تمثيل كافة أبعاد الدراسة بشكل دقيق من خلال مجموعة من الأسئلة القابلة للقياس حيث الوضوح في عملية القياس وتمثيل أبعاد الدراسة.

❖ اختيار صدق المقياس وثباته: تم اختيار صدق المقياس من خلال عرض

الاستبيان على عدد من المحكمين حيث تم تعديلها بناءً على مقترحاتهم.

❖ طرق المعالجة الإحصائية للمعلومات:

للإجابة على أسئلة الدراسة من خلال اختبار فرضيتها تم تفريغ البيانات وإخضاعها لمعالجات إحصائية مختلفة، باستخدام البرنامج الإحصائي (SPSS)، إذ تم استخدام الإحصاء الوصفي لإظهار النسب والتكرارات والانحراف المعياري لوصف ومقارنة أسئلة الدراسة، كما تم استخدام T (Test) لفحص الفرضيات والتحقق من صحتها، من خلال فحص الفروق بين المتوسطات ومعرفة ما إذا كانت هناك فروق ذات دلالة إحصائية. وتم دراسة العينات وذلك لمعرفة دور البنوك التجارية في مكافحة اختراقات أمن المعلومات.

#### • محددات البحث:

هذا البحث مثله مثل معظم البحوث اشتمل على مجموعة من المحددات سواء متعلقة بالمجالات أو المكان أو المدى الزمني للتطبيق وغيرها ومن المحددات:

- مجال التطبيق: نظراً لتعدد مجالات التطبيق في البنوك، فقد ركز هذا البحث على دور البنوك التجارية في مكافحة اختراقات أمن المعلومات.
- مكان التطبيق: نظراً لظروف الوقت مما يصعب معه القيام بالمسح الشامل لكل البنوك في المملكة العربية السعودية فإن هذا البحث ركز على أحد البنوك العريقة في مدينة جدة.
- مصدر المعلومات: أ - النوع الأول من البيانات والمعلومات تتمثل في المعلومات الثانوية وتم جمعها من الكتب والمقالات والأبحاث ومواقع الإنترنت. وذلك لوضع الإطار النظري للبحث.
- ب - النوع الثاني فهو قوائم الاستبيان التي جمعت من موظفي البنوك التجارية والعملاء.
- الفترة الزمنية والمدى الزمني للتطبيق: هذا البحث محدود بالفترة الزمنية التي تم خلالها القيام بالدراسة الميدانية وتجميع البيانات الأولية وهي الفصل الأول من العام الجامعي ٢٠١٠.

## رابعاً: اختبار الفروض

### المقدمة:

لتحليل وتفسير بيانات الدراسة تحليلاً علمياً يحقق أهدافها ويختبر فرضياتها واستخلاص أبرز نتائجها ، تم إدخال بيانات الدراسة في برنامج التحليل الإحصائي بالبرمجة الإحصائية للعلوم الاجتماعية (SPSS) وبعد معالجة بيانات الدراسة تم استخراج الجداول الإحصائية ، ومن ثم عرضها جدولياً وذلك لتفسير نتائجها .

وسيكون سيناريو تحليل البيانات وفق التصور التالي :

**أولاً:** عرض وتحليل البيانات الديموغرافية لعينة الدراسة.

**ثانياً:** اختبار صدق وثبات أداة الدراسة.

**ثالثاً:** نتائج اختبار الفرض الأول من الدراسة (مدى وجود اختراق لأمن المعلومات المصرفية)

**رابعاً:** نتائج اختبار الفرض الثاني للدراسة : تتباين عمليات اختراق أمن المعلومات بين المصارف التجارية كلا حسب قدراته التقنية وخبرات الموارد البشرية لديه.

**خامساً:** نتائج اختبار الفرض الثالث للدراسة (هناك علاقة بين أمن المعلومات والمستوى الثقافي والتعليمي للمستفيدين من الخدمة).

**سادساً:** نتائج اختبار الفرض الرابع للدراسة (وجود علاقة بين أداء وكفاءة وجاهزية المصارف التجارية ومخرجات أمن المعلومات المتمثلة في رضا العميل وحماية المعلومات الشخصية والمالية).

**سابعاً:** نتائج اختبار الفرض الخامس للدراسة (هناك علاقة طردية ذات دلالة إحصائية بين تقدم التقنية والقدرة على مكافحة سرية المعلومات).

ثامناً: نتائج اختبار الفرض السادس للدراسة (هناك علاقة بين أمن المعلومات وتعاون بعض موظفي البنوك في عملية الاختراق).

تاسعاً: نتائج اختبار الفرض السابع للدراسة (هناك علاقة بين قوة الإجراءات القانونية والقضائية والقدرة على مكافحة سرية أمن المعلومات).

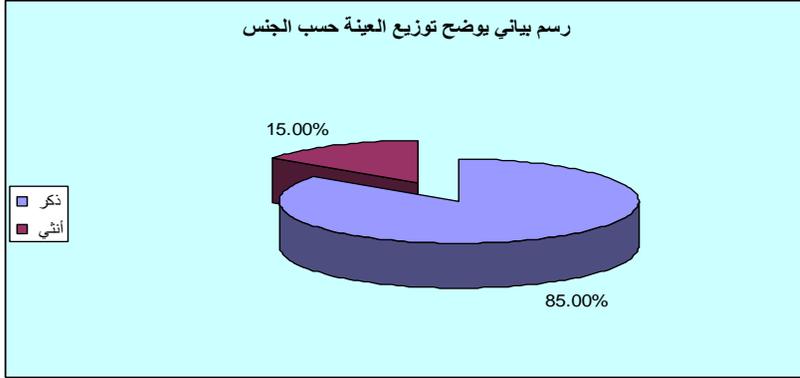
وفيما يلي نستعرض السيناريو السابق لتحليل بيانات الدراسة واختبار فرضياتها: أولاً: عرض وتحليل البيانات الديموغرافية لعينة الدراسة:

### جدول رقم (١)

#### توزيع عينة الدراسة تبعاً للجنس

النسبة المئوية	العدد	البيان
٪٨٥.٠	٥١	ذكر
٪١٥.٠	٩	أنثى
٪١٠٠	٦٠	المجموع

من الجدول رقم (١) أعلاه يتضح أن ٨٥٪ من أفراد العينة المشاركين في الدراسة هم ذكور، بينما بلغت نسبة الإناث ١٥٪. وعليه يستنتج مما سبق أن غالبية المشاركين في الدراسة هم ذكور وقد يعزى ضعف مشاركة الإناث في الدراسة المسحية في المملكة لأسباب اجتماعية تعرقل كيفية الوصول إلى العنصر النسائي، بالإضافة إلى ضعف وجود المرأة السعودية في بيئة العمل العامة.



شكل رقم (١) يوضح توزيع العينة حسب الجنس

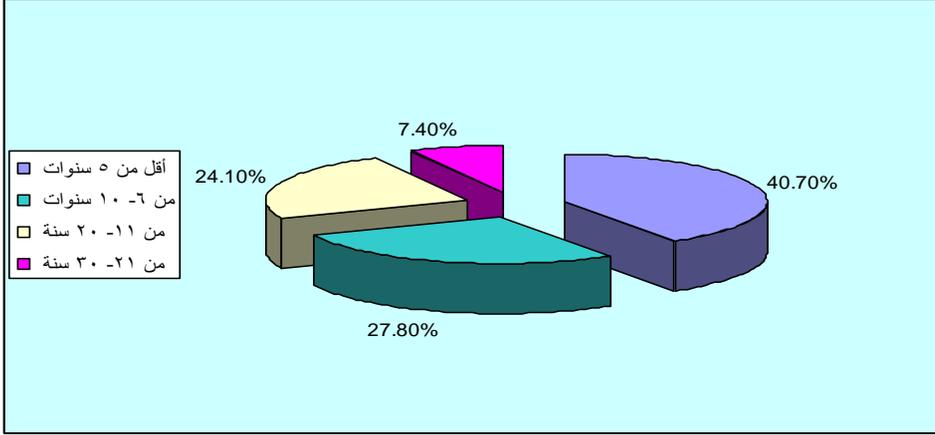
جدول رقم (٢)

توزيع عينة الدراسة تبعا لسنوات الخبرة

النسبة المئوية	العدد	البيان
٪٤٠.٧	٢٢	أقل من ٥ سنوات
٪٢٧.٨	١٥	من ٦ - ١٠ سنوات
٪٢٤.١	١٣	من ١١ - ٢٠ سنة
٪٧.٤	٤	من ٢١ - ٣٠ سنة
٪١٠٠	٥٤	المجموع

من الجدول رقم (٢) أعلاه يتضح أن ٤٠.٧٪ من أفراد العينة المشاركين في الدراسة سنوات خبرتهم أقل من ٥ سنوات ، بينما ٢٧.٨٪ تراوحت سنوات خبرتهم ما بين ٦ - ١٠ سنوات ، في حين أن ٢٤.١٪ تراوحت سنوات خبرتهم العلمية من ١١ - ٢٠ سنة ، كما أن من تراوحت سنوات خبرتهم من ٢١ - ٣٠ سنة بلغت ٧.٤٪ .

وعليه يستنتج مما سبق أن سنوات الخبرة لغالبية أفراد العينة أقل من ٥ سنوات وبالتالي قد لا يساعد ذلك في الكشف المبكر لعمليات اختراق أمن المعلومات البنكية .



شكل رقم (٢) توزيع العينة حسب سنوات الخبرة

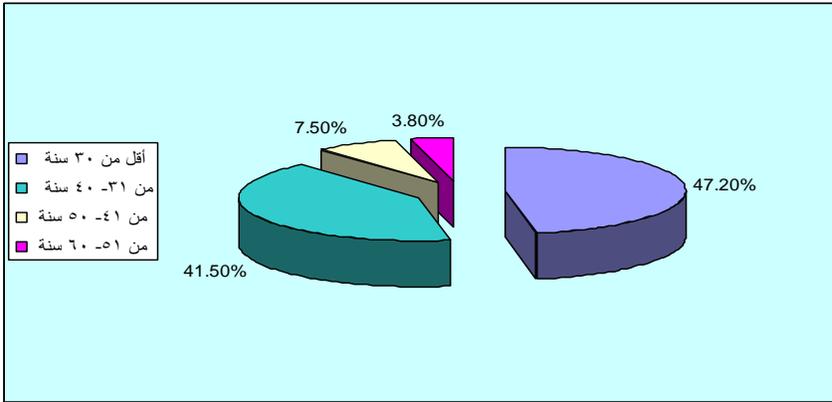
جدول رقم (٣)

توزيع عينة الدراسة تبعاً للعمر

النسبة المئوية	العدد	البيان
٪٤٧.٢	٢٥	أقل من ٣٠ سنة
٪٤١.٥	٢٢	من ٣١ - ٤٠ سنة
٪٧.٥	٤	من ٤١ - ٥٠ سنة
٪٣.٨	٢	من ٥١ - ٦٠ سنة
٪١٠٠	٥٣	المجموع

من الجدول رقم (٢) أعلاه يتضح أن أفراد العينة بنسبة ٤٧.٢٪ أعمارهم أقل من ٣٠ سنة ، بينما ٤١.٥٪ تراوحت أعمارهم ما بين ٣١ - ٤٠ سنة ، في حين أن ٧.٥٪ تراوحت أعمارهم ما بين ٤١ - ٥٠ سنة ، كما أن ٣.٨٪ تراوحت أعمارهم ما بين ٥١ - ٦٠ سنة .

وعليه يستنتج مما سبق الفئات العمرية لغالبية أفراد العينة جاءت من ٤٠ سنة فأقل حيث بلغت نسبتهم ٨٨.٧٪ . وبالتالي فإن هذه النتيجة تتسجم وتعزز قلة الخبرة العملية لأفراد العينة المشاركين في الدراسة في القطاع المصرفي .



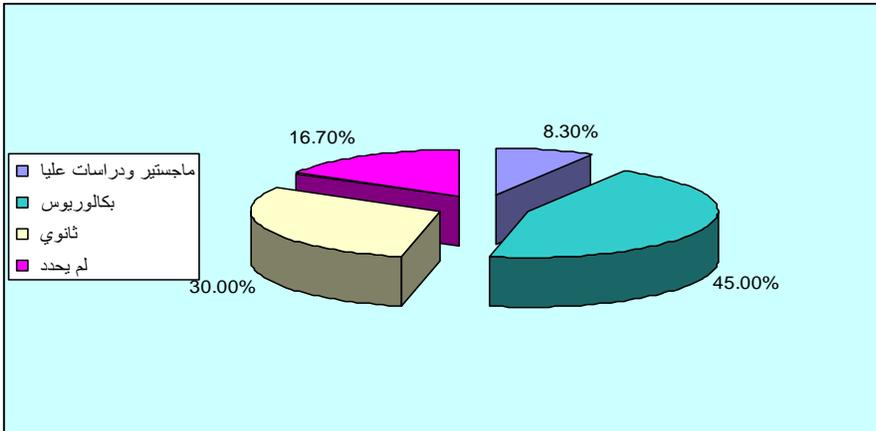
شكل رقم (٣) توزيع العينة حسب العمر جدول رقم (٤)

توزيع عينة الدراسة تبعا للمؤهل العلمي

النسبة المئوية	العدد	البيان
٨.٣٪	٥	ماجستير ودراسات عليا
٤٥.٠٪	٢٧	بكالوريوس
٣٠.٠٪	١٨	ثانوي
١٦.٧٪	١٠	لم يحدد
١٠٠٪	٦٠	المجموع

من الجدول رقم (٤) أعلاه يتضح أن أفراد العينة بنسبة ٨.٣٪ مؤهلاتهم العلمية ماجستير ودراسات عليا ، بينما ٤٥.٠٪ من أفراد العينة مؤهلاتهم العلمية بكالوريوس ، في حين أن ٣٠.٠٪ من حملة الشهادة الثانوية. كما يتبين من المؤشرات بالجدول أن ١٦.٧٪ لم يحددوا مؤهلاتهم العلمية .

وبالتالي يتبين أن غالبية أفراد العينة هم إما من حملة البكالوريوس أو حملة الشهادة الثانوية ، مما يعني أن تدريب هذه الفئات على عمليات اختراق أمن المعلومات ذو أهمية كبيرة لتحقيق الأمن المطلوب لحماية البيئة المصرفية من مخاطر هذا الاختراق .



شكل رقم (٤) توزيع العينة حسب المؤهل العلمي

ثانياً: اختبار صدق وثبات أداة الدراسة

١ - ثبات أداة الدراسة : تم قياس ثبات أداة الدراسة عن طريق معامل ألفا كرونباخ كما هو موضح بالجدول:

## جدول رقم (٥)

## Reliability Statistics

Cronbach's Alpha	N of Items
.899	45

من الجدول رقم (٥) أعلاه يتبين أن قيمة معامل ألفا كرونباخ بلغت (0.899) وهي قيمة عالية مما يعني أن أداة الدراسة تحقق ثباتا عاليا ، مما يعني سلامة إجراءات تصميم أداة الدراسة وتحقيق أهدافها المرجوة .

٢ - صدق أداة الدراسة : تم قياس صدق أداة الدراسة عن طريق معامل ارتباط محاور الدراسة مع المجموع الكلي لأداة الدراسة وذلك للتحقق من اتساق فقرات أداة الدراسة مع مجموعها الكلي ، كما هو موضح بالجدول التالي :

## جدول رقم (٦)

الدلالة الإحصائية	قيمة معامل الارتباط بيرسون	المحور
0.00	0.501**	وجود اختراق لأمن المعلومات
0.00	0.727**	تباين عمليات اختراق أمن المعلومات بين البنوك التجارية
0.00	0.814**	علاقة أمن المعلومات بالمستوى الثقافي والتعليمي للمستفيدين من الخدمة
0.00	0.794**	جودة أداء وكفاءة وجاهزية المصارف التجارية
0.001	0.450**	تقدم التقنية والقدرة على المكافحة
0.00	0.547**	أمن المعلومات وتعاون بعض موظفي البنوك في عملية الاختراق
0.00	0.736**	قوة الإجراءات القانونية والقضائية والقدرة على المكافحة

من الجدول رقم (٦) يتبين أن مجموع فقرات محاور الدراسة تحقق صدقا مرتفعا مع مجموعها الكلي مما يعني وجود ترابط واتساق جيد بين فقرات أداة الدراسة مما يطمئن الباحث إلى سلامة نتائج الدراسة .

ثالثا : نتائج اختبار الفرض الأول من الدراسة ( مدى وجود اختراق لأمن المعلومات البنكية ) .

## جدول رقم (٧)

## استجابات العينة نحو مدى وجود اختراق لأمن المعلومات البنكية

المتوسط الحسابي	لا أوافق بشدة		لا أوافق		محايد		موافق		موافق بشدة		العبارات
	ن	ت	ن	ت	ن	ت	ن	ت	ن	ت	
٢.٣٣	٤٠.٠%	٢٤	٢٠.٠%	١٢	١١.٧%	٧	٢٣.٣%	١٤	٥.٠%	٣	وجود اختراق لأمن المعلومات البنكية بصفة عامة
٢.٨٨	١٨.٣%	١١	٢٠.٣%	١٢	٢٥.٣%	١٢	٣٥.٦%	٢١	٥.١%	٣	أغلب عمليات الاختراق تتصف بعمليات اختراق داخلي
٢.٤٥	٢٩.٣%	١٧	٢٢.٤%	١٣	٢٥.٩%	١٥	١٩.٠%	١١	٣.٤%	٢	أغلب عمليات الاختراق تتصف بعمليات اختراق خارجي
٣.٣٨	١٠.٠%	٦	١٦.٧%	١٠	١٦.٧%	١٠	٣٨.٣%	٢٣	١٨.٣%	١١	يستطيع المخترق الداخلي أن يطلع على أرصدة عملاء البنك وأسراهم الشخصية
٣.٤٠	١٠.٠%	٦	١٣.٣%	٨	١٣.٣%	٨	٥٣.٣%	٣٢	١٠.٠%	٦	هناك بعض المخاطر التي تصاحب التعامل مع آلات الصرف الآلي
٣.٩٠	٢.٣%	٢	١٠.٠%	٦	١٦.٧%	١٠	٢٣.٣%	٢٠	٣٦.٧%	٢٢	أكثر وسائل الدفع الإلكتروني تعرضاً للاختلاس ، بطاقات الائتمان البنكية
٣.١٠	٦.٧%	٤	٣٠.٠%	١٨	٢١.٧%	١٣	٣٠.٠%	١٨	١١.٧%	٧	أكثر عمليات السرقة ( التقليدية ) للأموال تتم خلال عمليات الصرف الآلي
٣.٣٢	١.٧%	١	١٦.٩%	١٠	٣٩.٠%	٢٣	٣٢.٢%	١٩	١٠.٢%	٦	سرقة المعلومات الشخصية تعتبر من مخاطر أمن المعلومات، فعندما تكون

											حقوق الملكية الفردية موجودة في صيغة إلكترونية ومخزنة على الحاسب الآلي، فمن السهل سرقتها
٢.٦٥	%١٨.٣	١١	%٣٠.٠	١٨	%٢٦.٧	١٦	%١٨.٣	١١	%٦.٧	٤	يستطيع المخترق الخارجي أن يطلع على أرصدة عملاء البنك وأسراهم الشخصية
٣.٢٢	%٨.٥	٥	%١٣.٦	٨	%٣٧.٣	٢٢	%٢٨.٨	١٧	%١١.٩	٧	يستطيع المخترق الخارجي للنظام أن يعطل أنظمة الحاسوب كلياً
٣.٠٦	المتوسط الحسابي العام										

من الجدول رقم (٧) أعلاه والخاص بمدى وجود اختراق لأمن المعلومات البنكية فإن قيمة المتوسط الحسابي المرجح بلغت (٣.٠٦) تشير إلى أن الاتجاه العام لاستجابات العينة يميل نحو الحياد فيما يتعلق بوجود اختراق لأمن المعلومات البنكية .

كما يتبين من المؤشرات الواردة بالجدول السابق ما يلي :

١ - فيما يتعلق بمدى وجود اختراق لأمن المعلومات البنكية بصفة عامة يتضح أن أفراد العينة بنسبة ٦٠٪ جاءت استجاباتهم سلبية بشأن وجود اختراق لأمن المعلومات البنكية .

٢ - فيما يتعلق بأن أغلب عمليات الاختراق تتصف بعمليات اختراق داخلي، يتضح أن أفراد العينة بنسبة ٤٠.٦٪ يرون ذلك، بينما بلغت نسبة من لا يؤيدون ذلك ٣٨.٩٪ في حين بلغت نسبة المحايدون ٢٠.٣٪ .

٣ - فيما يتعلق بأن أغلب عمليات الاختراق تتصف بعمليات اختراق خارجي، فإن أفراد العينة بنسبة ٥١.٧٪ لا يؤيدون ذلك ، بينما ٢٢.٤٪ يرون ذلك، في حين بلغت نسبة المحايدون ٢٥.٩٪ .

- ٤ - فيما يختص بأن المخترق الداخلي يستطيع الإطلاع على أرصدة عملاء البنك وأسرارهم الشخصية ، فإن أفراد العينة بنسبة ٥٦.٦٪ جاءت استجاباتهم إيجابية ، بينما ٢٦.٧٪ استجاباتهم سلبية ، في حين أن ١٦.٧٪ محايدون .
- ٥ - فيما يتعلق بأن هناك بعض المخاطر تصاحب التعامل مع آلات الصرف الآلي ، يتبين أن أفراد العينة بنسبة ٦٣.٣٪ جاءت استجاباتهم إيجابية بخصوص ذلك ، بينما ٢٣.٣٪ يخالفون ذلك ، في حين أن ١٣.٣٪ محايدون .
- ٦ - كشفت النتائج بالجدول السابق بنسبة ٧٠.٠٪ بأن أكثر وسائل الدفع الإلكتروني تعرضا للاختلاس هي بطاقات الائتمان البنكية ، بينما ١٣.٣٪ لا يوافقون ، في حين أن ١٦.٧٪ محايدون .
- ٧ - فيما يتعلق بأن أكثر عمليات السرقة التقليدية للأموال تتم خلال عمليات الصرف فإن أفراد العينة بنسبة ٤١.٧٪ يؤيدون ذلك ، بينما ٣٦.٧٪ لا يوافقون ، في حين أن ٢١.٧٪ محايدون .
- ٨ - فيما يتعلق بأن سرقة المعلومات الشخصية تعتبر من مخاطر أمن المعلومات ، فإن أفراد العينة بنسبة ٤٢.٤٪ يؤيدون ذلك ، بينما ١٨.٦٪ لا يوافقون ، في حين أن ٣٩.٠٪ محايدون .
- ٩ - أظهرت النتائج في الجدول السابق أنه فيما يتعلق بأن المخترق الخارجي يستطيع أن يطلع على أرصدة عملاء البنك وأسرارهم الشخصية ، فإن أفراد العينة بنسبة ٢٥.٠٪ يؤيدون ذلك ، بينما ٤٨.٣٪ لا يوافقون ، في حين أن ٢٦.٧٪ محايدون .
- ١٠ - أظهرت النتائج في الجدول السابق أنه فيما يتعلق بأن المخترق الخارجي للنظام يستطيع أن يعطل أنظمة الحاسوب كلياً ، فإن أفراد العينة بنسبة ٤٠.٦٪

جاءت استجاباتهم إيجابية، بينما ٢٢.١٪ جاءت استجاباتهم سلبية أي لا يؤيدون ذلك، في حين أن ٣٧.٣٪ محايدون .

وبالتالي يستنتج من تفسير وتحليل فقرات محور اختراق أمن المعلومات البنكية أن من أبرز مظاهر هذا الاختراق تمثلت في مظهرين هما :

- أكثر وسائل الدفع الإلكتروني تعرضاً للاختلاس هي بطاقات الائتمان البنكية ويعزز ذلك قيمة المتوسط الحسابي لاستجابات العينة حيث بلغت (٣.٩٠) .

- هناك بعض المخاطر التي تصاحب التعامل مع آلات الصرف الآلي ويعزز ذلك المتوسط الحسابي المرجح حيث بلغت قيمته (٣.٤٠) .

## الفرض الثاني:

" تتباين عمليات اختراق أمن المعلومات بين البنوك التجارية كلا حسب قدراته التقنية وخبرات الموارد البشرية لديه "

## جدول رقم (٨)

استجابات العينة نحو مدى تباين عمليات اختراق امن المعلومات

بين البنوك التجارية كلا حسب قدراته التقنية وخبرات الموارد البشرية

المتوسط الحسابي	لا أوافق بشدة		لا أوافق		محايد		موافق		موافق بشدة		العبارات
	ن	ت	ن	ت	ن	ت	ن	ت	ن	ت	
٣.٧٣	٣	٢	١٣	٨	١١	٧	٥٠	٣٠	٢١	١٣	تساهم فرص التدريب على الحاسوب (في البنوك) في الحد من عمليات الاختراق
٤.٢٢	١	١	٠	٠	٦	٤	٥٨	٣٥	٣٣	٢٠	تعاون الإدارة العليا في البنوك يساهم في التقليل من عمليات الاختراق
٣.٩٠	٠	٠	١٠	٦	١٣	٨	٥٢	٣١	٢٣	١٤	عدم إلمام موظفي البنوك بالاستخدام الأمثل للتكنولوجيا الحديثة يؤدي إلى القصور في أداء العمليات الالكترونية بالشكل الصحيح
٤.١٥	٠	٠	١	١	١٥	٩	٤٩	٢٩	٣٣	٢٠	استخدام برامج غير ملائمة تحدث مخاطر وخلل في النظام
٤.٣٠	٢	٢	٣	٢	٥	٣	٣٦	٢٢	٥١	٣١	عدم إفصاح المعلومات عن العميل ( الاسم، العنوان، رقم الحساب، أرقام الهاتف ) يساهم في الحد من مخاطر أمن المعلومات
٣.٩٥	٣	٣	٣	٢	١٣	٨	٤٨	٢٩	٣٠	١٨	الزام البنوك بالإفصاح عن أي اختراق أمني لأنظمتها المعلوماتية قد يسبب حرج وفقدان كبير لثقة العملاء في البنوك
٣.٤٥	١	١	١١	٧	٣٠	١٨	٥٣	٣٢	٣	٢	عدم توافر القدرات العاملة المدربة

										تدريباً كاملاً على جوانب أمن المعلومات المختلفة مع الخطى المتسارعة لصناعة أنظمة وبرامج أمن وحماية المعلومات.	
٣.٢٤	%١.٧	١	%٢٥.٤	١٥	%٢٨.٨	١٧	%٣٥.٦	٢١	%٨.٥	٥	صعوبة توفر الأكفاء المختصين في أمن المعلومات يرجع إلى المهارات المتعددة المطلوبة لحماية المعلومات، وعدم نضج أنظمة وبرامج حماية المعلومات في الوقت الحالي
٣.٨٥	%٣.٣	٢	%٨.٣	٥	%١٦.٧	١٠	%٤٣.٣	٢٦	%٢٨.٣	١٧	خبرات موظفي البنك لها دور فعال في مكافحة عمليات اختراق سرية المعلومات
٣.٨٧	المتوسط الحسابي العام										

من الجدول رقم (٨) أعلاه والخاص بمدى تباين عمليات اختراق أمن المعلومات بين البنوك التجارية كلا حسب قدراته التقنية وخبرات الموارد البشرية لديه، فإن قيمة المتوسط الحسابي المرجح حيث بلغت (٣.٨٧) تشير إلى وجود توافق بين آراء العينة بأن عمليات اختراق أمن المعلومات بين البنوك التجارية كلاً حسب قدراته التقنية وخبرات الموارد البشرية. وعليه فإن هذه النتيجة تدعم صحة الفرض الثاني من الدراسة .

ومن أبرز أوجه تباين عمليات اختراق أمن المعلومات بين البنوك التجارية والمتعلقة بالقدرة التقنية وخبرات الموارد البشرية لدى البنوك مرتبة حسب درجة موافقة أفراد عينة الدراسة هي :

- ❖ عدم إفصاح المعلومات عن العميل ( الاسم، العنوان، رقم الحساب، أرقام الهاتف ) يساهم في الحد من مخاطر أمن المعلومات .
- ❖ تعاون الإدارة العليا في البنوك يساهم في التقليل من عمليات الاختراق .

- ❖ استخدام برامج غير ملائمة تحدث مخاطر واخلل في النظام .
- ❖ ألزام البنوك بالإفصاح عن أي اختراق أمني لأنظمتها المعلوماتية قد يسبب حرج وفقدان كبير لثقة العملاء في المصارف .
- ❖ عدم إلمام موظفي البنوك بالاستخدام الأمثل للتكنولوجيا الحديثة يؤدي إلى القصور في أداء العمليات الالكترونية بالشكل الصحيح .
- ❖ تساهم فرص التدريب على الحاسوب (في المصارف) في الحد من عمليات الاختراق .

ويعزز ذلك قيم المتوسطات الحسابية لاستجابات العينة حيث جاءت على التوالي:  
(٤.٣٠، ٤.٢٢، ٤.١٥، ٣.٩٥، ٣.٩٠) .

## الفرض الثالث:

" هناك علاقة بين أمن المعلومات والمستوى الثقافى والتعليمى للمستفيدين من الخدمة "

## جدول رقم (٩)

استجابات العينة نحو مدى وجود علاقة بين أمن المعلومات والمستوى الثقافى والتعليمى للمستفيدين من الخدمة

المتوسط الحسابي	لا أوافق بشدة		لا أوافق		محايد		موافق		موافق بشدة		العبارات
	ت	%ن	ت	%ن	ت	%ن	ت	%ن	ت	%ن	
٣.٨٢	٣	%٥.٠	٤	%٦.٧	١٠	%١٦.٧	٢٧	%٤٥.٠	١٦	%٢٦.٧	تساهم إجراءات التأمين على أموال العملاء بإحساسهم بالشعور بالرضا عن الخدمات المصرفية الإلكترونية
٤.٢٠	٣	%٥.٠	٣	%٥.٠	٤	%٦.٧	١٩	%٣١.٧	٣١	%٥١.٧	استخدام التقنية الحديثة (مثل الصراف الآلي) ساهم في امتلاك المصرف لشبكة من الفروع في شكل يتناسب مع تحقيق احتياجات العملاء باختلاف مناطقهم الجغرافية
٣.٩٣	٤	%٦.٨	٤	%٦.٨	٧	%١١.٩	٢١	%٣٥.٦	٢٣	%٣٩.٠	عدم اهتمام كثير من العملاء بأهمية سرية المعلومات مثل إعطاء الأرقام السرية للأقارب أو أي شخص في حالة عدم معرفة العميل باستخدام التقنية الحديثة (الصراف الآلي)
٣.٥٥	٤	%٦.٧	١١	%١٨.٣	٩	%١٥.٠	٢٠	%٣٣.٣	١٦	%٢٦.٧	طلب العميل المساعدة من موظف البنك وإعطائه حرية التعامل مع أرضه (العميل) مثل صلاحيات تداول بيع وشراء الأسهم ساهم في عمليات الاختلاس
٤.٢٧	١	%١.٧	٤	%٦.٨	٤	%٦.٨	١٩	%٣٢.٢	٣١	%٥٢.٥	العميل المتعلم أكثر حرصاً من العميل غير المتعلم
٣.٨٥	١	%١.٧	٣	%٥.١	١١	%١٨.٦	٢٣	%٥٥.٩	١١	%١٨.٦	هناك مخاطر أخرى يواجهها البنك مثل

											عدم تسديد حاملي البطاقات للديون المستحقة أو تحمل البنك نفقات ضياعها
٣.٤٠	%٦.٧	٤	%١٥.٠	٩	%٢٦.٧	١٦	%٣٥.٠	٢١	%١٦.٧	١٠	أخطاء العملاء في عدم قدرتهم للاستخدام الأمثل للتقنية الحديثة يؤدي إلى خسائر مالية للبنك
٣.٨٦	المتوسط الحسابي العام										

من الجدول رقم (٩) أعلاه والخاص هناك علاقة بين أمن المعلومات والمستوى الثقافى والتعليمى للمستفيدين من الخدمة ، فإن قيمة المتوسط الحسابى المرجح حيث بلغت ( ٣.٨٦ ) تشير إلى وجود توافق بين آراء العينة بان هناك علاقة بين أمن المعلومات والمستوى الثقافى والتعليمى للمستفيدين من الخدمة . وعليه فإن هذه النتيجة ترجح قبول الفرض الثالث من الدراسة .

ومما سبق نستنتج أن أمن المعلومات يرتبط بشكل مباشر بالمستوى الثقافى والتعليمى للمستفيدين من الخدمة ، وبالتالي فإن درجة ثقافة العملاء ومستوياتهم التعليمية لها دور مؤثر وحيوي في تحقيق أمن المعلومات وذلك لأن المستفيدين من الخدمة هم طرف أصيل في الحد من عمليات اختراق أمن المعلومات .

## الفرض الرابع :

" هناك علاقة بين جودة أداء وكفاءة وجاهزية المصارف التجارية ومخرجات أمن المعلومات المتمثلة في رضا العميل وحماية المعلومات الشخصية والمالية " .

## جدول رقم (١٠)

استجابات العينة نحو مدى وجود علاقة جودة أداء وكفاءة وجاهزية المصارف التجارية ومخرجات أمن المعلومات المتمثلة في رضا العميل وحماية المعلومات الشخصية والمالية

المتوسط الحسابي	لا أوافق بشدة		لا أوافق		محايد		موافق		موافق بشدة		العبارات
	ت	%ن	ت	%ن	ت	%ن	ت	%ن	ت	%ن	
٣.٥٥	٣	%٥.٠	٦	%١٠.٠	١٦	%٢٦.٧	٢٥	%٤١.٧	١٠	%١٦.٧	زيادة هجمات الفيروسات على مواقع البنوك، وتحولها من حالات مزعجة إلى ضارة بعمليات هذه البنوك، يلحق خسائر مادية كبيرة للبنوك
٣.٧٠	١	%١.٧	٨	%١٣.٣	١٥	%٢٥.٠	٢٠	%٣٣.٣	١٦	%٢٦.٧	المزايا التي تقدمها البنوك الالكترونية أفضل من المزايا التي تقدمها البنوك التقليدية من حيث الحماية المالية والشخصية للعميل
٣.٨٥	٣	%٥.٠	٥	%٨.٣	٧	%١١.٧	٢٨	%٤٦.٧	١٧	%٢٨.٣	ساهمت خدمة الاتصال الهاتفي في رضا العميل عن مستوى جودة الخدمات البنكية
٣.٨٨	١	%١.٧	٤	%٦.٧	١١	%١٨.٣	٢٩	%٤٨.٣	١٥	%٢٥.٠	تلعب التقنية الحديثة من أجهزة الحاسوب المتطورة دور كبير في الحد من عمليات اختراق سرية المعلومات
٤.١٧	٢	%٣.٣	١	%١.٧	٦	%١٠.٠	٢٧	%٤٥.٠	٢٤	%٤٠.٠	التقنية الحديثة تؤدي إلى التقليل من التكاليف المالية والوقت
٤.٢٤	١	%١.٧	٢	%٣.٤	٥	%٨.٥	٢٥	%٤٢.٤	٢٦	%٤٤.١	التقنية الحديثة تؤدي إلى إمكانية الوصول إلى قاعدة أوسع من العملاء

٤.١٢	%١.٧	١	%٦.٧	٤	%١٠.٠	٦	%٤١.٧	٢٥	%٤٠.٠	٢٤	التقنية الحديثة تؤدي إلى تقديم خدمات مصرفية كاملة وجديدة ذات كفاءة عالية
٤.٢٠	%١.٧	١	%١.٧	١	%٨.٣	٥	%٥١.٧	٣١	%٣٦.٧	٢٢	التقنية الحديثة تساهم في الاستفادة من الخدمات البنكية دولياً (السياحة الدولية)
٣.٩٨	%٠.٠	٠	%٦.٧	٤	%١٥.٠	٩	%٥١.٧	٣١	%٢٦.٧	١٦	ساهمت خدمة الصراف الآلي على إحساس العميل بالرضا عن مستوى جودة الخدمات البنكية
٣.٩٢	%٣.٣	٢	%٥.٠	٣	%١٨.٣	١١	%٤٣.٣	٢٦	%٣٠.٠	١٨	التقنية الحديثة تؤدي إلى السرعة والدقة في عمليات اتخاذ القرارات الإدارية
٣.٩٦	المتوسط الحسابي العام										

من الجدول رقم (١٠) أعلاه والخاص باستجابات العينة بأن هناك علاقة بين جودة أداء وكفاءة وجاهزية المصارف التجارية ومخرجات أمن المعلومات المتمثلة في رضا العميل وحماية المعلومات الشخصية والمالية فإن قيمة المتوسط الحسابي المرجح والتي بلغت ( ٣.٩٦ ) تشير إلى وجود توافق بين آراء العينة بأن هناك علاقة بين جودة وكفاءة وجاهزية المصارف التجارية ومخرجات أمن المعلومات المتمثلة في رضا العميل وحماية المعلومات الشخصية والمالية له . وعليه فإن هذه النتيجة ترجح قبول الفرض الرابع من الدراسة .

كما نستنتج من الجدول السابق أن أبرز مظاهر جودة وكفاءة وجاهزية المصارف التجارية في مواجهة مخاطر أمن المعلومات تمثلت فيما يلي :

- ❖ التقنية الحديثة تؤدي إلى إمكانية الوصول إلى قاعدة أوسع من العملاء
- ❖ التقنية الحديثة تساهم في الاستفادة من الخدمات المصرفية دولياً (السياحة الدولية)

- ❖ التقنية الحديثة تؤدي إلى التقليل من التكاليف المالية والوقت

- ❖ التقنية الحديثة تؤدي إلى تقديم خدمات مصرفية كاملة وجديدة ذات كفاءة عالية
- ❖ ساهمت خدمة الصراف الآلي على إحساس العميل بالرضا عن مستوى جودة الخدمات البنكية
- ❖ التقنية الحديثة تؤدي إلى السرعة والدقة في عمليات اتخاذ القرارات الإدارية

ويعزز ذلك قيم المتوسطات الحاسوبية لاستجابات العينة حيث جاءت على التوالي: (٤.٢٤، ٤.٢٠، ٤.١٧، ٤.١٢، ٣.٩٨، ٣.٩٢).

كما يستنتج مما سبق أن التقنية الحديثة هي عامل رئيسي في جودة وكفاءة وجاهزية المصارف التجارية في مواجهة مخاطر أمن المعلومات. ولذلك يتطلب ذلك من كافة البنوك التجارية الاستفادة من خيارات التقنية المتعددة وتدريب الموظفين على استخدامها في بيئة العمل المصرفي السعودي .

## الفرض الخامس :

" هناك علاقة طردية ذات دلالة إحصائية بين تقدم التقنية والقدرة على مكافحة سرية المعلومات".

## جدول رقم (١١)

استجابات العينة نحو مدى وجود علاقة بين تقدم التقنية والقدرة على مكافحة

## سرية المعلومات

المتوسط الحسابي	لا أوافق بشدة		لا أوافق		محايد		موافق		موافق بشدة		العبارات
	ت	%ن	ت	%ن	ت	%ن	ت	%ن	ت	%ن	
٣.٩٧	٣	٥.٠ %	٢	٣.٣ %	١٠	١٦.٧ %	٢٤	٤٠.٠ %	٢١	٣٥.٠ %	استخدام البنك لنظم سرية التشفير يساهم في التقليل من اختراق خصوصية الأفراد الشخصية ويساعد على سلامة المعلومات
٣.١٠	٦	١٠.٠ %	٦	١٠.٠ %	٢٨	٤٦.٧ %	١٦	٢٦.٧ %	٤	٦.٧ %	النقود الالكترونية سوف تحل مكان النقود التقليدية
٣.١٥	٣	٥.٠ %	٨	١٣.٣ %	٢٨	٤٦.٧ %	١٧	٢٨.٣ %	٤	٦.٧ %	بنوك الانترنت سوف تحل مكان البنوك التقليدية (على سبيل المثال مصرف اليابان نت)
٣.٤١	المتوسط الحسابي العام										

من الجدول رقم (١١) أعلاه والخاص باستجابات العينة بأن هناك علاقة بين تقدم التقنية والقدرة على مكافحة سرية المعلومات، فإن قيمة المتوسط الحسابي العام والتي بلغت (٣.٤١) تشير إلى أن أفراد العينة يوافقون على أن هناك علاقة بين تقدم التقنية والقدرة على مكافحة سرية المعلومات بالمصارف التجارية. ومن أبرز ما يمكن أن تستخدمه البنوك لتفعيل ذلك نظم سرية

التشفير حيث تساهم في التقليل من اختراق خصوصية الأفراد الشخصية ويساعد على سلامة المعلومات .

وعليه فإن النتيجة السابقة بشكل عام تدعم قبول الفرض الخامس من الدراسة حيث أن هناك علاقة بين تقدم التقنية والقدرة على مكافحة سرية المعلومات وذلك من خلال تطبيق النظم المتاحة حالياً بشكل فعال وتدريب الموظفين ورفع قدراتهم المهنية في مجال مكافحة عمليات الإضرار بالمعلومات البنكية .

كما يتبين من المؤشرات الواردة بالجدول أنه فيما يتعلق بأن النقود الإلكترونية سوف تحل مكان النقود التقليدية وأن بنوك الإنترنت سوف تحل مكان البنوك التقليدية فإن استجابات أفراد العينة تميل نحو الحياد ، حيث لا زال الوقت مبكراً للدخول إلى عالم الإلكترونيات بشكل كامل في مجال العمل المصرفي .

### الفرض السادس :

" هناك علاقة بين أمن المعلومات وتعاون بعض موظفي المصارف في عملية الاختراق " .

جدول رقم (١٢) استجابات العينة نحو مدى وجود علاقة بين أمن المعلومات

### وتعاون بعض موظفي المصارف في عملية الاختراق

المتوسط الحسابي	لا أوافق بشدة		لا أوافق		محايد		موافق		موافق بشدة		العبارات
	ت	%ن	ت	%ن	ت	%ن	ت	%ن	ت	%ن	
٣.٢٥	٣	%٥.٠	١٠	%١٦.٧	٢٠	%٣٣.٣	٢٣	%٣٨.٣	٤	%٦.٧	هناك علاقة بين الاختلاسات التي تتم داخلياً والتي تحصل للعملاء وتعاون بعض موظفي المصرف
٣.٠٣	٤	%٦.٧	١٣	%٢١.٧	٢٥	%٤١.٧	١٣	%٢١.٧	٥	%٨.٣	عمليات الاختراق الخارجي تتم بالتعاون مع بعض موظفي المصرف
٣.١٤	المتوسط الحسابي العام										

من الجدول رقم (١٢) أعلاه والخاص باستجابات العينة بأن هناك علاقة بين أمن المعلومات وتعاون بعض موظفي البنوك في عملية الاختراق ، فإن قيمة المتوسط الحسابي العام والتي بلغت ( ٣.١٤ ) تشير إلى أن استجابات أفراد العينة تميل نحو الحياد فيما يتعلق بوجود علاقة بين أمن المعلومات وتعاون بعض موظفي البنوك في عملية الاختراق .

وبالتالي فإن النتيجة السابقة لا تدعم قبول الفرض السادس من الدراسة ، وعليه لا توجد علاقة بين أمن المعلومات وتعاون بعض موظفي البنوك في عملية الاختراق. وبالتالي فإن مسألة تعاون بعض موظفي البنوك غير واردة بشكل أساسي في عملية الاختراق لأنه يمكن السيطرة على ذلك إدارياً وفنياً من خلال التقنية وأدوات الدخول والخروج إلى قاعدة معلومات العملاء أو قاعدة معلومات البنك .

### الفرض السابع :

" هناك علاقة بين قوة الإجراءات القانونية والقضائية والقدرة على مكافحة سرية أمن المعلومات".

جدول رقم (١٣) استجابات العينة نحو مدى وجود علاقة بين قوة الإجراءات القانونية والقضائية والقدرة على مكافحة سرية أمن المعلومات

المتوسط الحسابي	لا أوافق بشدة		لا أوافق		محايد		موافق		موافق بشدة		العبارات
	ت	%ن	ت	%ن	ت	%ن	ت	%ن	ت	%ن	
٣.٣٨	٤	٦.٧%	٧	١١.٧%	١٩	٣١.٧%	٢٢	٣٦.٧%	٨	١٣.٣%	القوانين القضائية غير حازمة في حماية حرمة الحياة الخاصة من الاعتداء عليها
٣.٤٢	٢	٣.٣%	٨	١٣.٣%	٢١	٣٥.٠%	٢١	٣٥.٠%	٨	١٣.٣%	عدم مواكبة القوانين القضائية المعمول بها مع التطور التقني في مجال المعلوماتية وأمن المعلومات
٣.٥٠	٢	٣.٣%	٩	١٥.٠%	١٥	٢٥.٠%	٢٥	٤١.٧%	٩	١٥.٠%	عدم تناسب القوانين المعمول بها مع

											الأنواع الجديدة من جرائم الحاسب الآلي
٣.٧٥	%٥.٠	٣	%٣.٣	٢	%١٦.٧	١٠	%٦١.٧	٣٧	%١٣.٣	٨	في حالة تواجد فروع لبنوك وطنية في دول أجنبية فإنه يجب أن تمارس قوانين الدول الأجنبية على هذه الفروع ويجب أن يطبق قانون دولي بصيغة موحدة متعارف عليها دولياً
٣.٥١	المتوسط الحسابي العام										

من الجدول رقم (١٣) أعلاه والخاص بأن هناك علاقة بين قوة الإجراءات القانونية والقضائية والقدرة على مكافحة سرية أمن المعلومات، فإن قيمة المتوسط الحسابي العام والتي بلغت (٣.٥١) تشير إلى أن أفراد العينة المشاركين في الدراسة يوافقون على وجود هذه العلاقة بين قوة الإجراءات القانونية والقضائية والقدرة على مكافحة سرية أمن المعلومات. وعليه فإن النتيجة السابقة تدعم قبول الفرض السابع من الدراسة، حيث تثبت النتيجة أن هناك علاقة جوهريّة بين قوة الإجراءات القانونية والقضائية والقدرة على مكافحة سرية أمن المعلومات في القطاع المصرفي.

### الفرض الثامن:

لا توجد فروق ذات دلالة إحصائية عند مستوى معنوية (0.05) بين استجابات عينة الدراسة نحو مدى وجود اختراق في أمن المعلومات البنكية يعزى لاختلاف متغيرات الدراسة (الجنس، سنوات الخبرة، العمر، والمؤهل التعليمي).

## جدول رقم (١٤) نتائج اختبار T-Test لدلالة الفروق في استجابات العينة نحو

## مدى وجود اختراق في أمن المعلومات المصرفية يعزى لاختلاف الجنس

مستوى الدلالة	قيمة $t$ المحسوبة	درجة الحرية	المتوسطات الحسابية		
			الجنس		
			أنثى	ذكر	
٠,١٨٢	١,٣٥	٥٨	١,٧٨	٢,٤٣	وجود اختراق لأمن المعلومات المصرفية بصفة عامة
٠,٣٩٤	٠,٨٥٩	٥٧	٢,٥٦	٢,٩٤	أغلب عمليات الاختراق تتصف بعمليات اختراق داخلي
٠,٥٥٨	- ٠,٥٩٠	٥٦	٢,٦٧	٢,٤١	أغلب عمليات الاختراق تتصف بعمليات اختراق خارجي
٠,٦٧٩	٠,٤١٦	٥٨	٣,٢٢	٣,٤١	يستطيع المخترق الداخلي أن يطلع على أرصدة عملاء المصرف وأسرارهم الشخصية
٠,١٥١	١,٤٥٦	٥٨	٢,٨٩	٣,٤٩	هناك بعض المخاطر التي تصاحب التعامل مع آلات الصرف الآلي
٠,٠٤٧	❖٢,٠٣	٥٨	٣,٢٢	٤,٠٢	أكثر وسائل الدفع الإلكتروني تعرضاً للاختلاس ، بطاقات الائتمان البنكية
٠,٩٧٥	- ٠,٠٣١	٥٨	٣,١١	٣,١٠	أكثر عمليات السرقة ( التقليدية ) للأموال تتم خلال عمليات الصرف الآلي
٠,٨٦٥	٠,١٧١-	٥٧	٣,٣٨	٣,٣١	سرقة المعلومات الشخصية تعتبر من مخاطر أمن المعلومات، فعندما تكون حقوق الملكية الفردية موجودة في صيغة إلكترونية ومخزنة على الحاسب الآلي، فمن السهل سرقتها
٠,٥١٣	- ٠,٦٥٨	٥٨	٢,٨٨	٢,٦١	يستطيع المخترق الخارجي أن يطلع على أرصدة عملاء البنك وأسرارهم الشخصية
٠,٩٩٦	٠,٠٠٦-	٥٧	٣,٢٢	٣,٢٢	يستطيع المخترق الخارجي للنظام أن يعطل أنظمة الحاسوب كلياً

تم احتساب قيمة  $T$  الجدولية عند مستوى معنوية (٠,٠٥) ودرجات حرية كما هو موضح بالجدول حيث بلغت ( ١,٦٥٨ )

المصدر : من إعداد الباحث استبانة الدراسة ٢٠١٠

- تعني أن هناك فروقاً ذات دلالة إحصائية عند مستوى معنوية (٠,٠٥) .

من الجدول رقم (١٤) أعلاه يتضح أن نتائج اختبار *T-TEST* قد كشفت عن وجود فروق ذات دلالة إحصائية عند مستوى معنوية (0.05) بين استجابات العينة تعزى لاختلاف الجنس فيما يتعلق بأن أكثر وسائل الدفع الإلكتروني تعرضا للاختلاس هي بطاقات الائتمان البنكية ، حيث تشير قيم المتوسطات الحسابية إلى أن الفروق تعود لصالح أفراد العينة الذكور حيث بلغ المتوسط الحسابي للذكور (٤,٠٢) مقابل متوسط حسابي للإناث بلغ (٣,٢٢)

### جدول رقم (١٥)

نتائج اختبار *F-Test* لدلالة الفروق في استجابات العينة نحو مدى وجود اختراق في أمن المعلومات البنكية يعزى لاختلاف سنوات الخبرة

مستوى الدلالة	قيمة F	درجة الحرية	سنوات الخبرة				
			المتوسطات الحسابية				
			٢١ - ٣٠	١١ - ٢٠	٦ - ١٠	أقل من ٥	
٠,٧٠٦	٠,٤٦٧	(٥٠, ٣)	١,٧٥	٢,٤٦	٢,٦٧	٢,٤٥	وجود اختراق لأمن المعلومات المصرفية بصفة عامة
٠,٧٤٠	٠,٤١٩	(٤٩, ٣)	٢,٢٥	٣,٠٠	٣,٠٠	٢,٩٥	أغلب عمليات الاختراق تتصف بعمليات اختراق داخلي
٠,٨٧١	٠,٢٣٦	(٤٨, ٣)	٢,٧٥	٢,٦٧	٢,٣٣	٢,٤٣	أغلب عمليات الاختراق تتصف بعمليات اختراق خارجي
٠,٦٦١	٠,٥٣٤	(٥٠, ٣)	٢,٧٥	٣,٦٢	٣,٥٣	٣,٣٢	يستطيع المخترق الداخلي أن يطلع على أرصدة عملاء البنك وأسراهم الشخصية
٠,٤١٣	٠,٩٧٣	(٥٠, ٣)	٤,٠٠	٣,٠٨	٣,٤٠	٣,٥٩	هناك بعض المخاطر التي تصاحب التعامل مع آلات الصرف الآلي
٠,١٥٨	١,٨٠٦	(٥٠, ٣)	١,٨٨	٢,٢٠	١,٨٩	١,٨٩	أكثر وسائل الدفع الإلكتروني تعرضاً للاختلاس ، بطاقات الائتمان البنكية
٠,١٣٦	١,٩٣٤	(٥٠, ٣)	٢,٥٩	٢,٨٩	٢,٣١	٢,٥٤	أكثر عمليات السرقة ( التقليدية ) للأموال تتم خلال عمليات الصرف الآلي
٠,١٣٤	١,٩٤٨	(٤٩, ٣)	٢,٢٣	٢,٣١	٢,٣٧	٢,٠٩	سرقة المعلومات الشخصية تعتبر من مخاطر أمن المعلومات، فعندما تكون حقوق الملكية الفردية موجودة في صيغة إلكترونية ومخزنة على الحاسب الآلي، فمن السهل سرقتها

٠,٩٠٨	٠,١٨٢	(٥٠, ٣)	١,٩٢	٢,٢٦	٢,٢٦	٢,٠٩	يستطيع المخترق الخارجي أن يطلع على أرصدة عملاء البنك وأسرارهم الشخصية
٠,٦٨٣	٠,٥٠١	(٤٩, ٣)	٢,٧٦	٢,٤٦	٢,٤١	٢,٦٩	يستطيع المخترق الخارجي للنظام أن يعطل أنظمة الحاسوب كلياً
تم احتساب قيمة $F$ الجدولية عند مستوى معنوية (٠,٠٥) ودرجات حرية كما هو موضح بالجدول أعلاه ؛ حيث بلغت قيمة $F$ (٢,٧٥).							

من الجدول رقم (١٥) يتضح أن نتائج اختبار  $F$  لم تكشف عن وجود أية فروق ذات دلالة إحصائية بين استجابات عينة الدراسة تعزى لاختلاف سنوات الخبرة فيما يتعلق بمدى وجود اختراق في أمن المعلومات البنكية ، ويعزز ذلك أن قيم  $F$  المحسوبة من بيانات العينة أقل من قيمة  $F$  الجدولية عند مستوى معنوية (0.05). وهذا يعنى أن هناك توافق بين آراء عينة الدراسة نحو وجود اختراق في أمن المعلومات البنكية باختلاف سنوات خبراتهم العملية .

جدول رقم (١٦) نتائج اختبار  $F$ -Test لدلالة الفروق في استجابات العينة نحو

مدى وجود اختراق في أمن المعلومات البنكية يعزى لاختلاف العمر

مستوى الدلالة	قيمة $F$	درجة الحرية	العمر				
			المتوسطات الحسابية				
			٦٠- ٥١	٥٠- ٤١	٤٠- ٣١	أقل من ٣٠	
٠,٥٥٤	٠,٧٠٥	(٤٩, ٣)	٢,٠٠	٣,٠٠	٢,٢٢	٢,٦٨	وجود اختراق لأمن المعلومات البنكية بصفة عامة
٠,٨٩٤	٠,٢٠٣	(٤٨, ٣)	٢,٥٠	٣,٢٥	٢,٩٥	٢,٨٣	أغلب عمليات الاختراق تتصف بعمليات اختراق داخلي
٠,٦٠١	٠,٦٢٨	(٤٧, ٣)	٢,٠٠	٣,٣٣	٢,٤١	٢,٥٤	أغلب عمليات الاختراق تتصف بعمليات اختراق خارجي
٠,٧٦٩	٠,٣٧٩	(٤٩, ٣)	٤,٠٠	٣,٠٠	٣,٥٠	٣,٢٨	يستطيع المخترق الداخلي أن يطلع على أرصدة عملاء البنك وأسرارهم الشخصية
٠,٤٧٤	٠,٨٤٨	(٤٩, ٣)	٤,٠٠	٣,٠٠	٣,٢٣	٣,٦٠	هناك بعض المخاطر التي تصاحب التعامل مع آلات الصرف الآلي
٠,٤٢٧	٠,٩٤٣	(٤٩, ٣)	٤,٥٠	٤,٧٥	٤,٠٠	٣,٩٢	أكثر وسائل الدفع الإلكتروني

							تعرضاً للاختلاس ، بطاقات الائتمان البنكية
٠,٠٣٠	٣,٢٣٩	(٤٩ ، ٣)	٢,٠٠	٢,٥٠	٢,٨٢	٣,٥٢	أكثر عمليات السرقة ( التقليدية ) للأموال تتم خلال عمليات الصرف الآلي
٠,٦٠٣	٠,٦٢٤	(٤٨ ، ٣)	٣,٥٠	٤,٠٠	٣,٣٦	٣,٣٣	سرقة المعلومات الشخصية تعتبر من مخاطر أمن المعلومات، فعندما تكون حقوق الملكية الفردية موجودة في صيغة إلكترونية ومخزنة على الحاسب الآلي، فمن السهل سرقتها
٠,٥٧٨	٠,٦٦٤	(٤٩ ، ٣)	٢,٥٠	٢,٧٥	٢,٣٢	٢,٨٠	يستطيع المخترق الخارجي أن يطلع على أرصدة عملاء البنك وأسرارهم الشخصية
٠,٣٤٩	١,١٢٣	(٤٨ ، ٣)	٢,٠٠	٣,٥٠	٣,١٤	٣,٣٨	يستطيع المخترق الخارجي للنظام أن يعطل أنظمة الحاسوب كلياً
تم احتساب قيمة $F$ الجدولية عند مستوى معنوية (٠,٠٥) ودرجات حرية كما هو موضح بالجدول أعلاه ؛ حيث بلغت قيمة $F$ (٢,٧٥)							

• تعني أن هناك فروقاً ذات دلالة إحصائية عند مستوى معنوية (٠,٠٥) .

من الجدول رقم (١٦) يتضح أن نتائج اختبار  $F$  عن وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة تعزى لاختلاف العمر فيما يتعلق بأن أكثر عمليات السرقة التقليدية للأموال تتم من خلال عمليات الصرف الآلي ويشير إلى ذلك قيمة  $F$  المحسوبة حيث جاءت أكبر من قيمة  $F$  الجدولية عند مستوى معنوية (٠,٠٥) . أما بقية فقرات اختراق أمن المعلومات البنكية فإن النتائج لم تشر إلى وجود أية فروق ذات دلالة إحصائية تعزى لاختلاف العمر لأفراد العينة .

جدول رقم (١٧) نتائج اختبار  $F$ -Test لدلالة الفروق في استجابات العينة نحو مدى وجود اختراق في أمن المعلومات البنكية يعزى لاختلاف المؤهل العلمي

مستوى الدلالة	قيمة $F$	درجة الحرية	المؤهل العلمي			
			المتوسطات الحسابية			
			ثانوي	بكالوريوس	ماجستير ودراسات عليا	
٠,٢٣٣	١,٥٠٥	(٤٧, ٢)	٢,٧٨	٢,٥٦	١,٦٠	وجود اختراق لأمن المعلومات البنكية بصفة عامة
٠,١٣٤	٢,١٠٠	(٤٦, ٢)	٣,٠٠	٣,٠٠	١,٨٠	أغلب عمليات الاختراق تتصف بعمليات اختراق داخلي
٠,٣٠١	١,٢٣	(٤٥, ٢)	٢,٧٦	٢,٤٤	١,٧٥	أغلب عمليات الاختراق تتصف بعمليات اختراق خارجي
٠,١٧٥	١,٨٠٧	(٤٧, ٢)	٣,٨٣	٣,١٩	٣,٠٠	يستطيع المخترق الداخلي أن يطلع على أرصدة عملاء البنك وأسرارهم الشخصية
٠,٨٨٩	٠,١١٨	(٤٧, ٢)	٣,٥٠	٣,٣٣	٣,٤٠	هناك بعض المخاطر التي تصاحب التعامل مع آلات الصرف الآلي
٠,٦١٦	٠,٤٨٩	(٤٧, ٢)	٣,٨٨	٤,٠٤	٤,٤٠	أكثر وسائل الدفع الالكتروني تعرضاً للاختلاس، بطاقات الائتمان البنكية
٠,٦٠٨	٠,٥٠٣	(٤٧, ٢)	٢,٨٣	٣,١٥	٣,٢٠	أكثر عمليات السرقة (التقليدية) للأموال تتم خلال عمليات الصرف الآلي
٠,٤٢٩	٠,٨٦٣	(٤٦, ٢)	٣,١٧	٣,٥٠	٣,٦٠	سرقة المعلومات الشخصية تعتبر من مخاطر أمن المعلومات، فعندما تكون حقوق الملكية الفردية موجودة في صيغة إلكترونية ومخزنة على الحاسب الآلي، فمن السهل سرقتها
٠,١٣٠	٢,١٣٤	(٤٧, ٢)	٣,٠٠	٢,٣٣	٢,٢٠	يستطيع المخترق الخارجي أن يطلع على أرصدة عملاء البنك وأسرارهم الشخصية
٠,٩٩٧	٠,٠٠٣	(٤٧, ٢)	٣,١٧	٣,١٩	٣,٢٠	يستطيع المخترق الخارجي للنظام أن يعطل أنظمة الحاسوب كلياً
تم احتساب قيمة $F$ الجدولية عند مستوى معنوية (٠,٠٥) ودرجات حرية كما هو موضح بالجدول أعلاه؛ حيث بلغت قيمة $F$ (٣,٢٣)						

من الجدول رقم (١٧) يتضح أن نتائج اختبار  $F$  لم تكشف عن وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة تعزى لاختلاف المؤهل العلمي فيما يتعلق بوجود اختراق في أمن المعلومات البنكية. وبالتالي هناك توافق بين آراء العينة فيما يتعلق بالوضع الراهن لاختراق أمن المعلومات البنكية.

## الجزء الخامس: نتائج وتوصيات البحث

### النتائج:

على ضوء تحليل وتفسير بيانات الدراسة الميدانية المتعلقة بأمن المعلومات وأثاره على أداء البنوك التجارية ، فقد توصلت الدراسة إلى النتائج التالية:

١ - حققت الدراسة معامل ثبات مرتفع حيث بلغت قيمة معامل ألفا كرونباخ (0.899) ، كما حققت معدلات صدق ذات دلالة إحصائية عند مستوى معنوية (0.05) وهذه المؤشرات تطمئن إلى سلامة إجراءات تصميم أداة الدراسة وبالتالي سلامة النتائج التي تتوصل إليها.

٢ - كشفت الدراسة أنه لا يوجد اختراق واضح لأمن المعلومات البنكية ، ويعزز ذلك أن استجابات عينة الدراسة تميل نحو الحياد حيث أن المتوسط العام لاستجابات أفراد العينة بلغت قيمته (3.06) . وعلى الرغم من ذلك فقد أوضحت الدراسة أن من أبرز مظاهر اختراق أمن المعلومات بالبنوك التجارية تتمثل في:

- أكثر وسائل الدفع الالكتروني تعرضاً للاختلاس هي بطاقات الائتمان البنكية .

- هناك بعض المخاطر التي تصاحب التعامل مع آلات الصرف الآلي .

٣ - كشفت الدراسة عن وجود تباين في عمليات اختراق أمن المعلومات بين البنوك التجارية كلا حسب قدراته التقنية وخبرات الموارد البشرية لديه . وعليه فإن هذه النتيجة تدعم صحة الفرض الثاني من الدراسة .

ومن أبرز أوجه تباين عمليات اختراق أمن المعلومات بين البنوك التجارية والمتعلقة بالقدرة التقنية وخبرات الموارد البشرية لدى البنوك مرتبة حسب درجة موافقة أفراد عينة الدراسة هي :

- ❖ عدم إفصاح المعلومات عن العميل ( الاسم، العنوان، رقم الحساب، أرقام الهاتف ) يساهم في الحد من مخاطر أمن المعلومات .
- ❖ تعاون الإدارة العليا في البنوك يساهم في التقليل من عمليات الاختراق .
- ❖ استخدام برامج غير ملائمة تحدث مخاطر وخلل في النظام .
- ❖ إلزام البنوك بالإفصاح عن أي اختراق أمني لأنظمتها المعلوماتية قد يسبب حرج وفقدان كبير لثقة العملاء في البنوك .
- ❖ عدم إلمام موظفي البنوك بالاستخدام الأمثل للتكنولوجيا الحديثة يؤدي إلى القصور في أداء العمليات الالكترونية بالشكل الصحيح .
- ❖ تساهم فرص التدريب على الحاسوب (في البنوك) في الحد من عمليات الاختراق .

٤ - أوضحت الدراسة أن هناك علاقة بين أمن المعلومات والمستوى الثقافى والتعليمى للمستفيدين من الخدمة ويعزز ذلك قيمة المتوسط الحسابى العام لاستجابات العينة حيث بلغت (٣.٨٦). وعليه فإن هذه النتيجة ترجح قبول الفرض الثالث من الدراسة . وبالتالي فإن درجة ثقافة العملاء ومستوياتهم التعليمية لها دور مؤثر وحيوي في تحقيق أمن المعلومات أو فشله وذلك لأن المستفيدين من الخدمة هم طرف أصيل في الحد من عمليات اختراق أمن المعلومات.

٥ - كشفت الدراسة أن هناك علاقة بين جودة أداء وكفاءة وجاهزية المصارف التجارية ومخرجات أمن المعلومات المتمثلة في رضا العميل وحماية المعلومات الشخصية والمالية ويشير إلى ذلك قيمة المتوسط الحسابي العام حيث بلغت (٣.٩٦) . وبناءً عليه فإن هذه النتيجة ترجح قبول الفرض الرابع من الدراسة .

٦ - بينت الدراسة أن من أبرز مظاهر جودة وكفاءة وجاهزية المصارف التجارية في مواجهة مخاطر أمن المعلومات تتمثل فيما يأتي:

- ❖ التقنية الحديثة تؤدي إلى إمكانية الوصول إلى قاعدة أوسع من العملاء
- ❖ التقنية الحديثة تساهم في الاستفادة من الخدمات البنكية دولياً (السياحة الدولية)

- ❖ التقنية الحديثة تؤدي إلى التقليل من التكاليف المالية والوقت
- ❖ التقنية الحديثة تؤدي إلى تقديم خدمات مصرفية كاملة وجديدة ذات كفاءة عالية

- ❖ ساهمت خدمة الصراف الآلي على إحساس العميل بالرضا عن مستوى جودة الخدمات البنكية

- ❖ التقنية الحديثة تؤدي إلى السرعة والدقة في عمليات اتخاذ القرارات الإدارية

٧ - أوضحت الدراسة أن هناك علاقة بين تقدم التقنية والقدرة على مكافحة سرية المعلومات، ويشير إلى ذلك قيمة المتوسط الحسابي العام والتي بلغت (٣.٤١) . وقد تبين أن من أهم ما يمكن أن تستخدمه البنوك التجارية لتفعيل ذلك استخدام نظم سرية التشفير حيث تساهم في التقليل من اختراق خصوصية الأفراد الشخصية ويساعد على سلامة المعلومات .

وعليه فإن النتيجة السابقة بشكل عام تدعم قبول الفرض الخامس من الدراسة حيث أن هناك علاقة بين تقدم التقنية والقدرة على مكافحة سرية المعلومات وذلك من خلال تطبيق النظم المتاحة حالياً بشكل فعال وتدريب الموظفين ورفع قدراتهم المهنية في مجال مكافحة عمليات الإضرار بالمعلومات البنكية .

٨ - بينت الدراسة أنه فيما يتعلق بأن النقود الإلكترونية سوف تحل مكان النقود التقليدية وأن بنوك الإنترنت سوف تحل مكان البنوك التقليدية فإن استجابات أفراد العينة تميل نحو الحياد ، حيث لا زال الوقت مبكراً للدخول إلى عالم الإلكترونيات بشكل كامل في مجال العمل المصرفي.

٩ - كشفت الدراسة أنه لا توجد علاقة بين أمن المعلومات وتعاون بعض موظفي البنوك في عملية الاختراق حيث أن الاتجاه العام لاستجابات العينة يميل نحو الحياد. وبالتالي فإن النتيجة السابقة لا تدعم قبول الفرض السادس من الدراسة.

١٠ - أوضحت الدراسة أن هناك علاقة بين قوة الإجراءات القانونية والقضائية والقدرة على مكافحة سرية أمن المعلومات، ويعزز ذلك قيمة المتوسط الحسابي العام والتي بلغت (٣.٥١).

وعليه فإن النتيجة السابقة تدعم قبول الفرض السابع من الدراسة ، حيث تثبت النتيجة أن هناك علاقة جوهرية بين قوة الإجراءات القانونية والقضائية والقدرة على مكافحة سرية أمن المعلومات في القطاع المصرفي .

١١ - كشفت نتائج اختبار *T-TEST* (جدول رقم -١٤) عن وجود فروق ذات دلالة إحصائية عند مستوى معنوية (0.05) تعزى لاختلاف الجنس بين استجابات

العينة أن أكثر وسائل الدفع الإلكتروني تعرضا للاختلاس هي بطاقات الائتمان البنكية .

١٢ - لم تكشف نتائج تحليل التباين الأحادي عن وجود فروق ذات دلالة إحصائية تعزى لاختلاف سنوات الخبرة بين استجابات العينة فيما يتعلق بوجود اختراق في أمن المعلومات البنكية .

١٣ - كشفت نتائج تحليل التباين الأحادي (اختبار  $F$ ) في جدول رقم ١٦- عن وجود فروق ذات دلالة إحصائية بين استجابات عينة الدراسة تعزى لاختلاف العمر فيما يتعلق بأن أكثر عمليات السرقة التقليدية للأموال تتم من خلال عمليات الصرف الآلي .

١٤ - أوضحت نتائج تحليل التباين في جدول رقم (١٧) أن نتائج اختبار  $F$  لم تكشف عن وجود فروق ذات دلالة إحصائية بين استجابات العينة تعزى لاختلاف المؤهل العلمي فيما يتعلق بوجود اختراق في أمن المعلومات البنكية .

### توصيات البحث:

- ❖ التأكيد على أهمية المعلومات الشخصية والمالية للعملاء والعمل على المحافظة على سريتها.
- ❖ مراقبة سلوك المعلومات من حيث حركتها وتجميعها وتداولها بين العملاء والعاملين في المصرف.
- ❖ إعطاء سلطات أكثر للإدارة العليا في المصارف (والتعاون مع الجهات الرسمية) للاطلاع على المعلومات الموجودة في الحواسيب الشخصية للعاملين فيها.
- ❖ في حالة عدم الرضا عن سلوك بعض الموظفين في المصرف يوضع الموظف تحت المراقبة الإلكترونية.
- ❖ التأكيد على التعاون الدولي في المجالات التالية:
  ١. الاستفادة من الخبرات الدولية في عمليات أمن المعلومات.
  ٢. إرسال موظفي المصارف والجهات الرسمية في دورات تدريبية إلى الخارج في مجال أمن المعلومات.
  ٣. نشر ثقافة الوعي المعلوماتي بين المواطنين والعاملين في المصارف، وطلاب الجامعات والشباب وربات البيوت وكبار السن.
  ٤. الربط بين الجامعات المحلية وجامعات الدول المتقدمة لعمل الأبحاث المشتركة في مجال أمن المعلومات.
  ٥. إنشاء شبكات اتصالات رسمية ودولية بين جميع الدول المعنية بأمن المعلومات لتوفير المعلومات المطلوبة وبأسرع وقت.

٦. تطبيق القانون في جميع الدول المعنية بأمن المعلومات في حالة حدوث الاختراق من أفراد في بلد ليست بلد المصرف.
٧. العمل على مجارية التغييرات التي تحدث في أنظمة شبكات الإنترنت والتعاون مع الدول المتقدمة وتوفير التقنيات الحديثة لمكافحتها.
٨. العمل على استحداث القوانين الجديدة التي تتناسب مع التغييرات المستمرة في مجال أمن المعلومات.
٩. إنشاء مركز للطوارئ مختص بالتعامل مع الأزمات في مجال أمن المعلومات والاستعداد لها مسبقاً.
١٠. إنشاء لجنة مكونة من أعضاء من جهات مختلفة مثل الجهات القضائية والطبية والمصرفية والأمن القومي ومندوب من سفارات الدول المعنية للمشاركة في الأمور المتشابكة والمعقدة.
١١. تطبيق العقوبات القانونية بكامل التفاصيل بحيث تتناسب مع نوعية الأعمال غير المشروعة.

## المراجع والمصادر العلمية

### المراجع العربية:

- ❖ بوادي حسنين، (٢٠٠٦)، إرهاب الانترنت الخطر القادم، الإسكندرية، دار الفكر الجامعي.
- ❖ داود حسن، (١٤٢٥)، أمن شبكات المعلومات، معهد الإدارة العامة، الرياض.
- ❖ زهيري طلال، الحاسوب الشخصي ومتطلبات امن المعلومات، الجامعة المستنصرية، بغداد.
- ❖ حجازي عبد الفتاح، (٢٠٠٦)، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الإسكندرية، دار الفكر الجامعي.
- ❖ حسيني صلاح، (٢٠٠٨)، أمن المعلومات لأنظمة المعلومات، بحث ماجستير غير منشور، بغداد،
- الرابط: <http://www.iraqstudent.net/detail.php?recordID=694>.
- ❖ جنبيهي منير وآخرون، (٢٠٠٥)، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، الإسكندرية، دار الفكر الجامعي.
- ❖ السعيد كامل، (١٩٩٣)، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، دار النهضة.
- ❖ شناوي مأمون، (٢٠٠٧)، جرائم الإنترنت وبطاقات الائتمان والجريمة المنظمة، القاهرة، دار الكتاب الحديث.
- ❖ شوابكة محمد، (٢٠٠٤)، جرائم الحاسوب والانترنت، عمان، دار المناهج.

- ❖ الشوا سامي، (١٩٩٤)، ثورة المعلومات وانعكاساتها على قانون العقوبات ، القاهرة ، دار النهضة العربية، ص ٤.
- عفيشات تيسير، (٢٠٠١)، أثر الجودة ورضا الزبون في تحديد الاستراتيجيات التسويقية للخدمة المصرفية، دراسة تحليلية على عينة من المصارف التجارية الأردنية، اطروحة دكتوراه، كلية الإدارة والاقتصاد، جامعة الموصل، العراق.
- ❖ عفيضي كامل، (٢٠٠٣)، جرائم الكمبيوتر، بيروت، منشورات الحلبي الحقوقية.
- ❖ عياد سامي، (٢٠٠٦)، الجريمة المعلوماتية وإجرام المعلوماتية، الإسكندرية، دار الفكر الجامعي .
- ❖ عبابنة محمود، (٢٠٠٥)، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع.
- ❖ مومني نهلا، (٢٠٠٨)، الجرائم المعلوماتية، عمان، دار الثقافة.
- ❖ مكاوي محمد، البيئة الرقمية بين سلبيات الواقع وآمال المستقبل، *Cybrarians Journal*، سبتمبر (2004).
- ❖ هيتي محمد، (٢٠٠٦)، جرائم الحاسوب، عمان، دار المناهج للنشر والتوزيع.
- ❖ ناجي محمد، (١٤٢٥)، نحو برنامج عملي لتنمية الدور الأمني للمؤسسات التربوية، ورقة عمل مقدمة لندوة المجتمع والأمن، كلية الملك فهد الأمنية، الرياض.
- ❖ نصيف عمر، (٢٠٠٩)، نظم المعلومات الإدارية ودورها في تحسين جودة الخدمات المصرفية، مجلة جامعة الأندلس، صنعاء، اليمن.
- ❖ ويكيديا، الموسوعة الحرة، (أمن المعلومات).

## المراجع الأجنبية:

- ❖ Anderson, K., "IT Security Professionals Must Evolve for Changing Market", SC Magazine, October 12, 2006.
- ❖ Aceituno, V., "On Information Security Paradigms", ISSA Journal, September, 2005.
- ❖ Dhillon, G., "Principles of Information Systems Security: text and cases", John Wiley & Sons, 2007.
- ❖ Rayport, J. F., and Sviokla, J. J., Managing in the Market space, Harvard Business Review, November-December 1994.

## الدوريات والمجلات:

- ❖ شبيب أنس، حماية المعلومات صارت مسألة حماية للاقتصاد الوطني، جريدة الشرق الأوسط، العدد ٩٢٩٢ تاريخ ٢١ ربيع الأول، سنة ١٤٢٥.