انعكاس جائحة كورونا علي نظم الرقابة الداخلية وأثرها علي أمن المعلومات بالبنوك التجارية المصرية " دراسة ميدانية "

إعداد

دكتور / نادر شعبان إبراهيم السواح

دكتور الفلسفة في المحاسبة

خبير تكنولوجيا المعلومات بالتربية والتعليم

انعكاس جائحة كورونا علي نظم الرقابة الداخلية وأثرها علي أمن المعلومات بالبنوك التجارية المصرية " دراسة ميدانية "

دكتور / نادر شعبان إبراهيم السواح

ملخص البحث

مع تعرض العالم لجائحة فيروس كورونا المستجد (COVID-19) بعد ظهوره في مدينة ووهان الصينية في سبتمبر ٢٠١٩ ، ومع استمرار تفشيه وتطوره، فمن الصعب التنبؤ بنطاق التأثير أو مدة التأثير في بيئة الأعمال وخاصة علي أمن المعلومات بعناصره الرئيسية المختلفة . ومن ثم فقد تنشئ هذه الظروف تحديات أمام المؤسسات المالية لحماية نظم المعلومات وقواعد البيانات وشبكات الاتصال الخاصة بها من الاختراق بسبب ضعف أنظمة الرقابة الداخلية نتيجة انتشار الفيروس والعمل في بيئة غير آمنة من الناحية التكنولوجية.

لذا فإن الفجوة البحثية تمثلت في ضرورة تحليل جميع الآثار الجوهرية لفيروس كورونا علي نظم الرقابة الداخلية وأثرها علي أمن المعلومات بالمؤسسات المالية ، بحيث يتيح للمتعاملين مع هذه المؤسسات معرفة المخاطر التي قد تتعرض لها وكيف يمكن التعامل معها .

تركز المشكلة البحثية علي تأثير جائحة كورونا علي أنظمة الرقابة الداخلية في بيئة الأعمال المصرفية وأثر ذلك علي أمن المعلومات بالمؤسسات المالية ، حيث أصبح من الأهمية بمكان تسليط الضوء على التداعيات والانعكاسات علي نظم الرقابة الداخلية في ظل انتشار فيروس كورونا واستخدام تكنولوجيا المعلومات والاتصالات في بيئة الأعمال المصرفية لحماية نظم المعلومات من الوصول غير المصرح به للمعلومات .

وبناء علي ما تقدم فإن الدراسة تهدف إلي ضمان حماية المعلومات من الأخطار الداخلية والخارجية ، و حماية سرية وسلامة وخصوصية محتوى المعلومات وحفظها من المخاطر المتعددة نتيجة انتشار وسائل وأدوات الاختراق والقرصنة على شبكة الإنترنت.

وانتهت الدارسة إلي أن هناك تأثير لجائحة كورونا علي نظام الرقابة الداخلية وتم تقييم تأثير ذلك علي أمن المعلومات بصورة عامة لبيان نقاط الضعف التي توجد في النظام وذلك للحد من وجودها بهدف تأمين النظام وضمان حماية أمن المعلومات المحاسبية.

Abstract

With the world exposed to the new Corona virus (COVID-19) pandemic after its appearance in the Chinese city of Wuhan in September 2019, and with its continued spread and development, it is

difficult to predict the scope of the impact or the duration of the impact on the business environment, especially on information security with its various main elements. Hence, these circumstances may create challenges for financial institutions to protect their information systems, databases and communication networks from penetration due to weak internal control systems as a result of the spread of the virus and work in an environment that is technologically insecure.

Therefore, the research gap was represented in the necessity to analyze all the essential effects of the Corona virus on internal control systems and its impact on the information security of financial institutions, in order to allow those dealing with these institutions to know the risks they may be exposed to and how they can be dealt with.

The research problem focuses on the impact of the Corona pandemic on internal control systems in the banking environment and its impact on information security in financial institutions, as it has become extremely important to highlight the implications and implications for internal control systems in light of the spread of the Corona virus and the use of information and communication technology in the banking environment, to protect information systems from unauthorized access to information.

Based on the foregoing, the study aims to ensure the protection of information from internal and external dangers, and to protect the confidentiality, integrity and privacy of information content and its preservation from multiple risks as a result of the spread of hacking and piracy means and tools on the Internet.

The study concluded that there is an impact of the Corona pandemic on the internal control system, and the impact of that on information security in general was evaluated to indicate the weaknesses that exist in the system in order to limit its presence in order to secure the system and ensure the protection of the accounting information security.

أولا : المقدمة:-

أصبحت نظم المعلومات وقواعد البيانات وشبكات الاتصال عصب العالم المعرفي والصناعي والمالي والصحي والاجتماعي وغيرها من القطاعات. حيث أصبح من المهم الحفاظ علي أمن المعلومات بعناصره الرئيسية. إلا أنه يوجد العديد من المخاطر التي تواجه أمن المعلومات التي يمكن أن تؤدي إلي خسائر جوهرية إذا تم تجاهلها . حيث اشارت إحدى الدراسات إلى أن قيمة

أعمال الجرائم الإلكترونية أصبحت تُقدر بحوالي 105 بليون دولار سنويًا، وهذا الرقم يفوق قيمة أعمال تجارة المخدرات في جميع أنحاء العالم [١].

وعلي المستوي العالمي أصدرت المنظمة الدولية للمعايير (ISO) مجموعة من المعايير الخاصة بأمن المعلومات تعرف بـ ISO 27K ، وهي سلسلة من المعايير أصدرتها المنظمة الدولية للمعايير (ISO) وتم تطويرها بالتعاون مع اللجنة الكهروتقنية الدولية (IEC) ، والتي تهدف الى تقديم إرشادات بشأن الممارسات الجيدة لأنظمة إدارة أمن المعلومات المصممة لحماية سرية وسلامة وتوافر محتوى المعلومات ونظم المعلومات مثل (ISO/IEC 27001 - ISO/IEC 27002 - ISO/IEC 27016 - ISO/IEC 27038) . كما أصدرت جمعية الرقابة والمراجعة على نظم المعلومات (ISACA) النسخة الخامسة من إطار العمل COBIT5 لتوفير التوجيه اللازم وضمان وجود مستوى معين من الحماية للمعلومات [٢] .

ونظرا لتعرض العالم لجائحة عالمية متمثلة في انتشار فيروس كورونا المستجد (COVID-19) بعد ظهوره في مدينة ووهان الصينية في سبتمبر ٢٠١٩ ، ومع استمرار تفشيه وتطوره، فمن الصعب التنبؤ بنطاق التأثير أو مدة التأثير في بيئة الأعمال وخاصة علي أمن المعلومات بعناصره الرئيسية المختلفة . ومن ثم، قد تخلق هذه الظروف تحديات أمام المؤسسات المالية لحماية نظم المعلومات وقواعد البيانات وشبكات الاتصال الخاصة بها من الاختراق بسبب ضعف أنظمة الرقابة الداخلية والتي قد يسببها انتشار الفيروس والعمل في بيئة غير آمنة من الناحية التكنولوجية بسبب الإجراءات الاحترازية في التعامل مع الفيروس . لذا فإن الفجوة البحثية تمثلت بضرورة تحليل جميع الآثار الجوهرية لفيروس كورونا علي نظم الرقابة الداخلية وأثرها علي أمن المعلومات بالمؤسسات المالية. بحيث يتيح للمتعاملين مع هذه المؤسسات معرفة المخاطر

---

[١] - نقلا عن :
أ.م. علي مال الله عبد الله ، د. خالص حسن الناصر ، " حوكمة أمن المعلومات ودورها في تخفيض مخاطر نظم المعلومات المحاسبية الالكترونية " ، " ورقة عمل مقدمة الى الندوة العلمية لقسم إدارة الاعمال كلية الإدارة والاقتصاد جامعة الموصل بالتعاون مع قيادة عمليات نينوى الموسومة" الإدارة الأمنية في محافظة نينوى " وسبل تطويرها " ، ديسمبر ٢٠١٩ ،ص ٢ .

[2] - A- Kris Seeburn ," COBIT as an It Governance Mechanism ", IT Governance Institute 2008 and ISACA Serving IT Governance Professionals , P 11.

B - T. Olzak, (2013), "COBIT 5 for Information Security: The Underlying Principles",www.techrepublic.com View publication .

التي قد يتعرض لها عند التعامل معها من خلال تكنولوجيا الاتصالات وكيف يمكن التعامل معها .

ثانيا : مشكلة البحث :

إن توجه المؤسسات المصرفية إلي تقديم الخدمات المصرفية من خلال استخدام شبكات عامة مثل الانترنت ، أحدث نقلة جذرية في صناعة الخدمات المالية والمصرفية . ولكن لا يخفي في ذات الوقت أن المؤسسات المالية قد أدركت بأن تلك الفوائد والخدمات التي تتيحها شبكة الانترنت قد تتضمن مخاطر عديدة منها :-

- زيادة إمكانية حدوث عمليات الاحتيال المالي نتيجة غياب المعايير والمبادئ الفعالة التي يمكن الاستناد عليها للتحقق والتثبت من هوية العملاء والمتعاملين في اطار الطبيعة المفتوحة لشبكة الإنترنت.
- بروز قضايا انتهاك الخصوصية بشكل متزايد في العمليات المالية والمصرفية الإلكترونية وذلك في ضوء ما تتضمنه هذه العمليات من مراحل متعددة لتجميع وانتقال متكرر للمعلومات والبيانات .

ولذلك تزايدت أهمية تطبيق أمن المعلومات وذلك لضمان حماية المعلومات من التهديدات الداخلية والخارجية ، و حماية سرية وسلامة وخصوصية محتوى المعلومات وحفظها من المخاطر المتعددة نتيجة انتشار وسائل وأدوات الاختراق والقرصنة على شبكة الإنترنت ، ومكافحة أنشطة الاعتداء علي المعلومات أو استغلال أنظمتها لارتكاب الجرائم الإلكترونية .

و نظرا للتغيرات التي وقعت في بيئة الأعمال والمتمثلة في انتشار فيروس كورونا وآثاره علي أمن المعلومات للمؤسسات المالية ، أصبح من الأهمية بمكان تسليط الضوء على التداعيات والانعكاسات علي نظم الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات والاتصالات في بيئة الأعمال وخاصة المصرفية منها و التي أحدثها انتشار فيروس كورونا علي تطبيق الوسائل المختلفة لحماية نظم المعلومات من الاختراق بهدف تدمير أو تغير أو الاستخدام الغير أخلاقي للبيانات والمعلومات الخاصة بالمتعاملين مع هذه المؤسسات .

وبناء على ذلك يمكن صياغة مشكلة البحث بالتساؤل الآتي : ماهي انعكاسات تفشي فيروس كورونا علي نظم الرقابة الداخلية وأثر ذلك علي أمن المعلومات بالبنوك التجارية ؟ ويتفرع عنه عدة أسئلة فرعية هي :

- ماهي عناصر و وسائل أمن المعلومات بالبنوك التجارية ؟
- هل يوجد علاقة ارتباط جوهرية بين انعكاسات تفشي فيروس كورونا علي نظم الرقابة الداخلية و أمن المعلومات بالبنوك التجارية ؟

- هل يوجد تأثير جوهري لانعكاسات تفشي فيروس كورونا لنظم الرقابة الداخلية علي أمن المعلومات بالبنوك التجارية ؟

ثالثا : أهمية البحث :

لا تزال الاستجابة العالمية لتفشي جائحة فيروس كورونا تتطور بسرعة منذ مطلع العام 2020 ، ومع استمرار تفشيه وتطوره ، واتخاذ الدول للتدابير الاحترازية اللازمة للحد من انتشاره ، وظهور بعض الأثار السلبية علي تطبيق كافة الوسائل اللازمة لحماية الوصول غير المرخص للبيانات والمعلومات الخاصة بالمؤسسات المالية . لذلك تكمن أهمية البحث في تحليل ومناقشة أهم العوامل التي توثر علي أمن المعلومات في البنوك التجارية المصرية في ظل تفشى فيروس كورونا المستجد .

رابعا : حدود الدراسة :

- يتمثل مجتمع الدراسة في العاملين بإدارات تكنولوجيا المعلومات بالبنوك التجارية المصرية .
- عينة الدراسة : العاملين بإدارات تكنولوجيا المعلومات في بعض البنوك المصرية وهم بنك مصر ، والقاهرة ، و البنك الأهلي المصري .
- قام الباحث بتصميم الاستقصاء الخاص بالدراسة الميدانية وذلك اعتمادا علي المتغيرات البحثية التي ثبت جدواها واختبارها إحصائيا والواردة بالجهود البحثية بالدراسات السابقة المعروضة بالدارسة .

خامسا : أهداف الدارسة :

تهدف هذه الدراسة إلى:

- بيان التهديدات والمخاطر المحتملة التي يمكن أن يتعرض لها أمن نظم المعلومات وما قد ينجم عن ذلك من أضرار وخسائر جسيمة، و ذلك استنادا الى الادبيات ذات العلاقة.
- التعرف علي أثر تفشي فيروس كورونا علي أمن المعلومات للمؤسسات المالية مع زيادة كل من التهديدات الداخلية والخارجية وذلك بسبب اتباع بعض الإجراءات الاحترازية وما يترتب عليها من ضعف نظام الرقابة الداخلية لهذه المؤسسات .
- إظهار أهمية تحديد التهديدات ذات العلاقة بأمن نظم المعلومات كخطوة تمهيدية ضرورية لتشخيص نقاط الضعف في أنظمة الرقابة والحماية الخاصة بتلك النظم ومعالجتها.

سادسا : منهجية البحث :

اعتمد الباحث علي المنهجين الاستقرائي والاستنباطي كما يلي :-

المنهج الاستقرائي :

ومن خلاله قام الباحث بتحديد إطار لأبعاد مشكلة البحث وأهدافه ، حيث تناول التأصيل العلمي لأبعاد المشكلة وذلك بالاعتماد علي الكتب العلمية والمقالات والأبحاث المنشورة والدوريات المختلفة المرتبطة بموضوع البحث وذلك بهدف معرفة أثر جائحة كورونا علي أمن المعلومات في بيئة الأعمال المصرية.

المنهج الاستنباطي :

ومن خلاله قام الباحث باختبار فروض البحث وتحديد مدي قبول هذه الفروض من عدمه، وتقييم الأثر الناتج عن فيرس كورونا علي نظم الرقابة الداخلية وأثر ذلك علي أمن المعلومات في البنوك التجارية المصرية ولذلك قام الباحث بإعداد قائمة الاستقصاء المناسبة لجمع البيانات المتعلقة بنطاق البحث لإمكان وضع فروض الدراسة في صورة قابلة للاختبار الإحصائي . كما قام الباحث باستخدام تحليل التباين ANOVA وأسلوب تحليل الارتباط Correlation وأسلوب تحليل الانحدار المرحلي Stepwise regression لاختبار الفروض البحثية.

سابعا : فروض البحث :

تقوم الدارسة علي فرضية أساسية وهي : إن انتشار فيروس كورونا عالميا سينعكس أثره علي أمن المعلومات في المؤسسات المالية من خلال التأثير علي نظم الرقابة الداخلية لهذه المؤسسات . و ينبثق عن هذه الفرضية الفروض الفرعية التالية :-

١- لا توجد اختلافات ذات دلالة إحصائية بين متوسط آراء عينات الدراسة للبنوك الثلاثة علي انعكاسات تفشي فيروس كورونا علي نظم الرقابة الداخلية وأثرها علي أمن المعلومات بالبنوك التجارية .
٢- لا يوجد علاقة ارتباط جوهرية بين انعكاسات تفشي فيروس كورونا علي نظم الرقابة الداخلية و أمن المعلومات بالبنوك التجارية.
٣- لا يوجد تأثير جوهري لانعكاسات تفشي فيروس كورونا لنظم الرقابة الداخلية علي أمن المعلومات بالبنوك التجارية .

ثامنا : الدراسات السابقة :

دراسة : صدام محمد محمود ، وأخرون ٢٠٢٠ [١]

هدفت هذه الدراسة إلي بيان أهم التعديلات التي يمكن أن تحصل في الممارسات المحاسبية المعتمدة في إعداد التقارير المالية كنتيجة عن الآثار الاقتصادية التي أحدثها فيروس كورونا على مستوى العالم، وكان من أهم ما خلصت إليه الدراسة ما يلي :

---

[١] - أ.د/ صدام محمد محمود ، أ.د/علي إبراهيم حسن ، " تداعيات الأزمات والنوازل المجتمعية علي الممارسات المحاسبية فيروس كورونا (COVID-19) أنموذجا دراسة نظرية تحليلية " ، جامعة تكريت ، كلية الإدارة والاقتصاد ، مجلة تكريت للعلوم الإدارية والاقتصادية ، المجلد (١٦) العدد (٤٩) ج١ ، ٢٠٢٠ ، ص ١- ٢٤ .

- اعتبار الأحداث الناتجة عن تداعيات الفيروس ضمن التقارير المالية المعدة في ٢٠١٩/١٢/٣١ على أنها أحداثا غير قابلة للتعديل وفقا لمتطلبات المعيار الدولي (IAS10) ، ورغم ذلك كان هناك توجهات بضرورة الإفصاح عن البنود غير المعدلة والتي ستتأثر بشدة بالآثار الاقتصادية عن تداعياته مستقبلا ، واعتبارها أحداثا قابلة للتعديل ضمن التقارير المالية في ٢٠٢٠/١٢/٣١ .
- على الرغم من كثرة وشدة الانتقادات الموجهة للمعيار الدولي (IFRS9)، والمطالبة بإيقاف تطبيقه أو على الأقل تعديل بعض فقراته، إلا أن مجلس معايير المحاسبة الدولية (IASB) أوصى بعدم إيقافه وعدم إجراء أي تعديل عليه خلال الفترة الحالية ،على اعتبار أن فيه من المرونة التي تؤهله لاستيعاب الآثار الناتجة عن تفشي الفيروس.
- قد يواجه المراجعون صعوبة في الوصول إلى الأدلة والأشخاص الذين يحتاجون إليهم لدعم رأيهم في عملية المراجعة ، وقد يؤدي هذا الأمر إلى اضطرارهم للكشف عن قيود النطاق لإجراءاتهم المعتادة ضمن تقاريرهم.

دراسة : الوليد أحمد طلحة ٢٠٢٠ [١]

هدفت هذه الدراسة إلي تحليل الأثر الاقتصادي للانتشار فيروس كورونا علي مستوي الدول العربية ، وكان من أهم ما خلصت إليه الدراسة ما يلي :

- أن فيروس كورونا قد أثر بصورة مباشرة على عدد من الجوانب والقطاعات الاقتصادية وقد كان التأثير علي جانبي الطلب والعرض معا. و يتطلب ذلك استجابة واسعة على صعيد السياسات النقدية والمالية لدعم الطلب وتوفير التمويل اللازم للقطاعات المختلفة والأكثر تضرراً من تفشي فيروس كورونا.
- رغم أن السياسات النقدية التحفيزية سوف تساعد على تحفيز الطلب الكلي في الاقتصاد من خلال تحفيز النمط الاستهلاكي وتشجيع الاستثمار، إلا أنه يتعين على الحكومات العربية أن تحترز من تداعيات ذلك على موازناتها وعلى أوضاع القطاع الخارجي وعلى أسعار صرف عملاتها وعلى تدفقات رؤوس الأموال.

[١] - د . الوليد أحمد طلحة ، " التداعيات الاقتصادية لفيروس كورنا المستجد علي الدول العربية " ، صندوق النقد العربي ، إبريل ٢٠٢٠ ، ص ١-٤٥ .

- لا يزال هناك قدر كبير من عدم اليقين بشأن الآثار الاقتصادية المحتملة لفيروس كورونا الا أن التوقعات تشير الى أن الصدمة قد تكون كبيرة بالأخص فيما يتعلق بتوفير مدخلات الإنتاج والسلع الاستهلاكية المستوردة.

دراسة : شوقي فوده ، وأخرون ٢٠١٩[١].

تهدف هذه الدارسة إلي دراسة أثر فاعلية أمن نظم المعلومات المحاسبية الإلكترونية في تحسين ربحية البنوك التجارية المصرية ، وتوصلت هذه الدراسة إلي أنه يوجد تأثير ذو دلالة إحصائية لفاعلية أمن نظم المعلومات المحاسبية علي تحسين ربحية البنوك التجارية المصرية .

دراسة : نزار إبراهيم قويدر ٢٠١٨ [٢]

تهدف هذه الدارسة إلي التعرف علي أثر نظم الرقابة الداخلية علي أمن المعلومات المطبق بشركة المدار للهاتف المحمول وتحديد متغيراتها والعلاقة بينها وتحديد نقاط الضعف بإجراءات الرقابة المطبقة داخل الشركة واقتراح السبل الناجحة لضمان رفع مستوي أمن معلومات الشركة. وكان من أهم نتائجها:

- تؤثر إجراءات الرقابة التنظيمية المطبقة بالشركة علي أمن المعلومات من خلال وجود فصل واضح للوظائف بين مختلف الإدارات وتوفير أجهزة إنذار وكاميرات مراقبة واستخدام كلمات مرور خاصة وسرية .
- يتمتع القائمون علي نظام الرقابة الداخلية بالخبرة والكفاءة اللازمة للحفاظ علي أمن المعلومات بالشركة ، كما يتمتع القائمون علي نظام الرقابة الداخلية بالاستقلالية اللازمة للحفاظ علي أمن المعلومات بالشركة .
- **دراسة : ISACA, 2013 [٣].**

هدفت هذه الدراسة إلى وضع إطار عمل لإدارة أمن المعلومات المحاسبية الإلكترونية وأظهر هذا الإطار عدة مجالات تتمثل في : حوكمة برامج أمن المعلومات عن طريق إدارة خطر المعلومات ، وتطوير برامج أمن المعلومات ، وإدارة برامج أمن المعلومات ، وطرق الاستجابة لمخاطر أمن المعلومات .

---

[١] - أ.د/ شوقي فوده ، دينا الدسوقي ، " أثر العلاقة بين فاعلية أمن نظم المعلومات المحاسبية الإلكترونية وربحية البنوك التجارية المصرية مع دراسة تطبيقية " ، مجلة الدراسات التجارية المعاصرة ، كلية التجارة – جامعة كفر الشيخ ، العدد السابع يونيو ٢٠١٩ ، ص ٥٩٥ ، ٦٢٤ .

[٢] - نزار إبراهيم قويدر ، (نظم الرقابة الداخلية وأثرها علي أمن المعلومات " دراسة ميدانية علي شركة المدار للهاتف المحمول ") ، المجلة الجامعة - كلية الاقتصاد والعلوم السياسية – جامعة طرابلس ، العدد العشرون – المجلد الثاني – اكتوبر – ٢٠١٨ ، ص ١ -٤٠ .

[3] - Information Systems Audit and Control Association (ISACA), "COBIT 4.1 Framework for IT Governance and Control", Available at: www.isaca.org, Accessed: 25 May, 2014.

وكان من أهم نتائج هذه الدراسة ضرورة قيام المؤسسات بتطبيق تلك المجالات للوصول لمجموعة من العوامل التي تساعد علي تفعيل و نجاح برامج أمن المعلومات . وايضا وجود مجموعة من العوامل الهامة التي تؤثر في نجاح برامج أمن المعلومات مثل : فهم الإدارة لإصدارات أمن المعلومات والتخطيط المسبق لبرامج أمن المعلومات .

دراسة : Al-Hanini,2012 [1] .

تهدف هذه الدارسة إلي التعرف علي مخاطر نظم المعلومات المحاسبية الإلكترونية في البنوك الأردنية ، والتعرف علي أسباب وطرق الوقاية من هذه المخاطر .

وتوصلت هذه الدراسة إلي أن هناك مخاطر تهدد أمن المعلومات المحاسبية في البنوك الأردنية وذلك نتيجة نقص خبرة الموظفين في حفظ أمن المعلومات ، والتي تتمثل في عدم تدريب الموظفين علي استخدام وسائل حماية النظم المحاسبية قبل البدء ، وعدم وجود أنظمة التعيين المناسبة والتي تقضي بتعيين الشخص المناسب في المكان المناسب .

دراسة : رشا حمادة ٢٠١٠ [٢]

تناولت هذه الدارسة الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية وأثرها في زيادة موثوقية المعلومات المحاسبية . ولتحقيق أهداف الدراسة قام الباحث بعمل استبيان تم توزيعه علي مكاتب المراجعة للحسابات في مدينة دمشق ، وقد تضمن الاستبيان الضوابط الرقابية العامة الأربعة لنظم المعلومات المحاسبية الإلكترونية وهي الضوابط التنظيمية ، وضوابط الرقابة علي الوصول ، ضوابط أمن وحماية الملفات ،و وضوابط تطوير وتوثيق النظام ، وذلك من حيث أثرها في زيادة موثوقية المعلومات المحاسبية في الشركات .

وقد خلصت الدارسة إلي أن هناك تأثيرا كبيرا للضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية في الشركات .

دراسة : Abu-Musa , 2010 [٣] .

---

[1] - Al-Hanini, Eman (2012), " The Risks of Using Computerized Accounting Information Systems in the Jordanian Banks: Their Reasons and Ways of Pre-vention", European Journal of Business and Management, Vol. 4, No. 20 .

[٢] - رشا حمادة ، " أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية " ، مجلة جامعة دمشق الاقتصادية والقانونية – المجلد ٢٦ – العدد الاول ، ٢٠١٠ .

3 - Abu-Musa, Ahmad A. (2010), "Information security Governance in Saudi Organization: An Empirical Study " Pubic Administration, A Professional Quarterly Journal Published by the Institute of Public Administration Riyadh, Saudi Arabia.

سعت هذه الدراسة إلى اختبار وجود وتطبيق حوكمة أمن المعلومات في المنظمات السعودية وهدفت إلي تقييم الوضع الحالي والملامح الرئيسية لحوكمة أمن نظم المعلومات المحاسبية الإلكترونية في بيئة العمل السعودي ، من خلال دراسة سرية المعلومات في المنظمات السعودية .

وكان من أهم نتائج هذه الدراسة أنه علي الرغم من أهمية حوكمة أمن المعلومات كعامل مكمل لنجاح تكنولوجيا المعلومات و حوكمة الشركات ، فإنه لم يتم التعرف بوضوح علي الأدوار والمسئوليات الخاصة بأمن المعلومات ، كما أن المنظمات السعودية ليس لديها استراتيجيات أو سياسات أمن للمعلومات واضحة ومكتوبة ، وليس لديها خطط واضحة للتعامل مع مخاطر أمن المعلومات .

دراسة : عطا الله أحمد الحسبان ٢٠٠٩[١]

هدفت هذه الدراسة إلى تحديد مدي تعامل مراجعي أنظمة تكنولوجيا المعلومات في المصارف التجارية مع معايير المراجعة الدولية ذات العلاقة بأمن وسرية المعلومات وأثرها علي بقاء البنوك التجارية وتحقيق الأهداف العامة لها.

وكان من أهم نتائج هذه الدارسة أن المراجعين يتعاملون بمتطلبات الأمن والسرية الخاصة بالبنوك ، وتحافظ علي تغييرها باستمرار من وقت لآخر بدرجة متوسطة من حيث التخطيط والتوجيه وتقييم المخاطر .

ومن أهم ما وصت به هذه الدراسة ضرورة عمل الندوات والدورات المستمرة لمراجعي أنظمة تكنولوجيا المعلومات حول أهمية ونوعية وطبيعة وطرق أمن المعلومات ، وأيضا ضرورة تجديد المعلومات الخاصة بالشركة حسب مستجدات أدوات تكنولوجيا المعلومات ومحاولة تحسين قواعد البيانات للبنوك من وقت لآخر .

دراسة : صلاح الدين الهيتي ، وأخرون ٢٠٠٥ [٢]

هدفت هذه الدراسة إلى التعرف على أثر التهديدات الأمنية بمصادرها الداخلية والخارجية في أمن المعلومات بنتائجها المباشرة وغير المباشرة في ضوء تطبيق الحكومة الإلكترونية، حيث تم إجراء دراسة ميدانية في عدد من الوزارات الأردنية وأمانة عمان الكبرى.

---

[١] - عطا الله أحمد الحسبان ، " مدي تعامل مدققي أنظمة تكنولوجيا المعلومات بمعايير التدقيق الخاصة ببيئة أنظمة المعلومات للمحافظة علي أمن وسرية المعلومات في البنوك الأردنية " ، مجلة كلية بغداد للعلوم الاقتصادية الجامعة – العدد العشرون – أ ، ٢٠٠٩ .

[٢] - صلاح الدين الهيتي ، وأمنة ماجد الربيحات ، "أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية: دراسة ميدانية في عدد من الوزارات الأردنية وأمانة عمان الكبرى"، مجلة المحاسبة والإدارة والتأمين، جهاز الدراسات العليا والبحوث، كلية التجارة، جامعة القاهرة، العدد ٦٥، (٢٠٠٥)، ص ٣٠٩-٣٧٨.

و قد خلصت الدراسة إلى ضرورة التنبه إلى خطورة التهديدات الداخلية على أمن المعلومات وتوفير سياسة أمنية تحافظ على الموثوقية والخصوصية والتكاملية لكل منظمة تسعى إلى المحافظة على النظام المعلوماتي بأكمله لدعم نجاح الحكومة الإلكترونية.

دراسة : أحمد عبد السلام أبو موسى ٢٠٠٤ (١)

سعت هذه الدراسة إلي اختبار المخاطر الرئيسية والهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشآت السعودية.

وأشارت الدراسة إلى أن هناك العديد من المخاطر التي يتعرض لها أمن هذه النظم في المنشآت السعودية، من أبرزها الإدخال غير المتعمد والمتعمد للبيانات من قبل موظفي المنشأة ، والتدمير غير المتعمد والمتعمد للبيانات من قبل موظفي المنشأة ، واشتراك الموظفين في استخدام نفس كلمات السر، وإدخال فيروسات إلى النظام .

دراسة : Kankanhalli, Atreyi et al 2003 (٢)

هدفت هذه الدارسة إلى تطوير نموذج متكامل للفاعلية الأمنية لنظام المعلومات واختباره عملياً.

و كان من أهم ما توصلت إليه هذه الدارسة أن المنظمات الصغيرة والمتوسطة الحجم تمارس أنشطة رادعة أقل من المنظمات الكبيرة الحجم لضمان أمن نظام المعلومات ، وتزداد الإجراءات الوقائية في المنظمات التي تدعم إدارتها العليا نظام المعلومات مقارنة مع المنظمات التي لا تدعم إدارتها العليا نظام المعلومات ، وتطبق المنظمات المالية إجراءات مشددة على أمن المعلومات أكثر من بقية المنظمات ، وأن الجهود الرادعة والوقائية لحماية المعلومات تعزز الفاعلية الأمنية لنظام المعلومات.

دراسة : أحمد عبد السلام أبو موسى ٢٠٠٢ (٣)

تناولت هذه الدراسة المخاطر الرئيسية التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية وكفاية أنظمة الحماية المطبقة في البنوك المصرية.

---

١ - أحمد عبد السلام أبو موسى ، "أهمية مخاطر المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المنشآت السعودية"، المجلة العلمية للتجارة والتمويل، كلية التجارة، جامعة طنطا، العدد الثاني، (٢٠٠٤)، ص ٦-٥٤.

2 - Kankanhalli, Atreyi et al., "An Integrative Study of Information Systems Security effectiveness," International Journal of Information Management, Vol. 23, (2003) PP. 139-154.

٣ - أحمد عبد السلام أبو موسى ، " جرائم الكمبيوتر: هل يمكنك حماية نظام المعلومات المحاسبية الخاصة بك؟ " ، بحوث مؤتمر الاقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية، عمان، الأردن، ٢٠٠٢، ص ٦٠٩-٦٢٥.

وكان من نتائج هذه الدراسة أن الإدخال غير المتعمد لبيانات غير صحيحة من قبل موظفي البنوك ، والتدمير غير المتعمد للبيانات من قبل الموظفين، وإدخال فيروس الحاسوب إلى النظام، والكوارث الطبيعية، والكوارث من صنع الإنسان، واشتراك الموظفين في استخدام نفس كلمة السر، وتوجيه البيانات والمعلومات إلى أشخاص غير مخول لهم باستلامها، تُعد من أهم المخاطر التي تواجه أمن النظم المذكورة. كما قدمت الدراسة بعض المقترحات لتلافي نقاط ضعف أنظمة الحماية في قطاع البنوك المصري.

موقع الدراسة الحالية من الدراسات السابقة :

١- تناولت الدراسات السابقة أهم أنواع المخاطر والتهديدات التي تتعرض لها أنظمة المعلومات وخاصة المعلومات المحاسبية .
٢- أن ضعف أنظمة الرقابة الداخلية هو ما قد يؤدي إلي وجود ثغرات ونقاط ضعف تؤدي إلي وجود التهديدات والمخاطر الداخلية والخارجية .
٣- أن المخاطر والتهديدات الداخلية تعد من أكثر المخاطر التي تتعرض لها المؤسسات وخاصة المالية منها .
٤- أن فيروس كورونا قد أثر بصورة مباشرة على كل مناحي الحياة الاقتصادية ، والصحية ، والاجتماعية وغيرها .
٥- أن فيروس كورونا قد أثر بصورة مباشرة على عدد من الجوانب والقطاعات الاقتصادية وقد كان التأثير علي جانبي الطلب والعرض معا.

وتسعي الدارسة الحالية إلي دراسة تأثير جائحة كورونا علي أمن المعلومات بصورة عامة ، ومدي تأثير ذلك علي نظام الرقابة الداخلية للمؤسسات المالية وذلك لبيان نقط الضعف التي يمكن أن تحدث في حال تطبيق الإجراءات الاحترازية وذلك للحد من والوصول غير المرخص للبيانات والمعلومات الخاصة بهذه المؤسسات في ظل تفشي فيروس كورونا .

تاسعا : خطة البحث :

تحقيقا للأهداف التي يسعي إليها البحث وللإجابة عن التساؤلات المطروحة واختبار مدي صحة فروض الدراسة الميدانية، فقد أمكن تنظيم خطة البحث في خمسة محاور بخلاف الإطار العام وذلك علي النحو التالي :

المحور الأول : نبذة عامة عن جائحة كورونا.

المحور الثاني : الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات وأثر جائحة كورونا عليها .

المحور الثالث : ماهية أمن المعلومات

المحور الرابع : عناصر ووسائل أمن المعلومات .
المحور الخامس : الدراسة الميدانية .
نتائج وتوصيات الدراسة.

المحور الأول : نبذة عامة عن جائحة كورونا.

يختلف فيروس كورونا عن باقي الأوبئة والأمراض التي أصابت العالم على مر التاريخ، التي انحصر تفشيها في نطاق جغرافي محدود حول العالم أو دولة بعينها مثل وباء سارس في الصين، ووباء إيبولا في غرب أفريقيا، والإنفلونزا الإسبانية، وإنفلونزا الخنازير، حيث لم تترك هذه الأمراض والأوبئة نفس الأثر الذي نتج عن فيروس كورونا خلال فترة قصيرة [١] .

المحور الثاني: الرقابة الداخلية في ظل استخدام تكنولوجيا المعلومات وأثر جائحة كورونا عليها .

يتناول هذا المحور العناصر التالية :
أولا :- مفهوم نظام الرقابة الداخلية .
ثانيا : تأثير تكنولوجيا المعلومات علي الرقابة الداخلية .
ثالثا : تأثير نظام الرقابة الداخلية علي تكنولوجيا المعلومات.
رابعا:أهمية نظام الرقابة الداخلية في ظل التشغيل الإلكتروني للبيانات.
خامسا : مقومات نظام الرقابة الداخلية في ظل التشغيل الإلكتروني للبيانات .
سادسا :- مخاطر تكنولوجيا المعلومات .
سابعا : أثر جائحة كورونا علي تطبيق عناصر الرقابة الداخلية في بيئة التشغيل الإلكتروني للبيانات . كما يلي :

أولا :- مفهوم نظام الرقابة الداخلية :-

يقع علي عاتق إدارة المؤسسة تصميم نظام للرقابة الداخلية يستهدف مواجهة أو تقليل المخاطر التي يترتب عليها انتهاك خصوصية البيانات والمعلومات والاستخدام الضار لها في غير صالح المؤسسة وعملائها .

[١] - د/ الوليد أحمد طلحه ، " التداعيات الاقتصادية لفيروس كورونا المستجد علي الدول العربية " ، صندوق النقد العربي ، إبريل ٢٠٢٠ ، ص ٥ .

و لا تختلف أهداف نظام الرقابة الداخلية في ظل النظام الإلكتروني للبيانات عنه في ظل النظام المحاسبي اليدوي حيث يهدف نظام الرقابة الداخلية إلي تحقيق وظيفتين رئيسيتين هما [1] :-

الأولي : حماية موارد المؤسسة من سوء الاستخدام .

و يطلق عليها الرقابة المانعة أو الوقائية أو الرقابة قبل الأداء و هي تمثل الرقابة المحاسبية . و توضع هذه الرقابة لمنع حدوث عدم الكفاءة.

الثانية: تنمية الكفاءة الإنتاجية في المنشأة و ضمان تحقيق السياسات و الأهداف التي و ضعتها إدارة المؤسسة .

و يطلق عليها الرقابة بالتغذية المرتدة لأنها تبدأ بعد انتهاء الرقابة الوقائية كما يطلق عليها أيضا الرقابة الإدارية أو الرقابة بعد الأداء حيث يتم إعداد تقارير الأداء و يتم مقارنة الأداء الفعلي مع المخطط و تحديد مقدار الانحراف و في ضوء ذلك يتم تصحيح تلك الانحرافات .

و يلاحظ هنا أنه توجد علاقة وثيقة بين هاتين الوظيفتين للرقابة الداخلية حيث يكون من الصعب الفصل بينهما حيث لا يمكن تحقيق الكفاءة الإنتاجية في المنشأة بدون حماية مواردها من سوء الاستخدام و هذا ما أكده المجمع الأمريكي في " نشرة معايير المراجعة رقم (١) "

و يمكن تعريف الرقابة الداخلية علي أنها [2] " مجموعة السياسات و الإجراءات المتكاملة و التي تضعها إدارة المنشأة و تكون مسئولة عن متابعة تنفيذها من خلال العاملين لديها و ذلك لتوفير تأكيد معقول بتحقيق أهداف المنشأة الموضوعة بمعرفة إدارة المنشأة من قبل و تهدف إلي تحقيق:

- حماية موارد المؤسسة من سوء الاستخدام .
- إمكانية الاعتماد علي التقارير و القوائم المالية .
- تحقيق الكفاءة و الفاعلية علي مستوي كافة أنشطة المنشأة .
- تشجيع السير بالسياسات الإدارية في الطريق المرسوم لها ."

و نظرا لتباين طبيعة مشكلات الرقابة الداخلية في ظل التشغيل الإلكتروني للبيانات عنه في ظل النظام اليدوي فسوف ينعكس أثر هذا التباين علي أهداف الرقابة الداخلية ،ويمكن تلخيص أهم أهداف الرقابة الداخلية في بيئة التشغيل الإلكتروني كما يلي:-

---

[1] - ستيفن أ. موسكو ف. مارك ج – سيمكن . ترجمة د/ كمال الدين سعيد " نظم المعلومات المحاسبية لاتخاذ القرارات "، المملكة العربية السعودية : جامعة الملك سعود ، كلية الاقتصاد والإدارة فرع القصيم ، ١٩٨٤، ص ٢٣٨ .

[2] - د/ سناء الدين فوزي ، وآخرون ، " أساسيات مراجعة الحسابات "، كلية التجارة – جامعة طنطا ، الطبعة الأولي ٢٠٠٢ ، ص ٢١٥-٢١٦ .

- التأكد من تشغيل كل البيانات الواجب تشغيلها .
- التأكد من أنه لم يحدث أي تغير في هذه البيانات أثناء مراحل التشغيل المختلفة.
- التأكد من عدم التدخل غير المصرح به أثناء مراحل التشغيل .
- التأكد من تحديد البيانات غير الصحيحة وتحديد الإجراءات اللازمة للتعامل معها.
- التأكد من صحة المخرجات و توزيعها علي الأشخاص المصرح لهم بذلك فقط.
- التأكد من أن النظام يعمل بطريقة عالية من الكفاءة و بأسلوب فعال .

و قد أثرت هذه الأهداف علي وسائل تحقيق مفهوم و مقومات الرقابة الداخلية في بيئة التشغيل الإلكتروني للبيانات،ولكن مع ملاحظة أن مكونات وإجراءات الرقابة الداخلية لا تختلف في بيئة التشغيل الإلكتروني للبيانات عنها في بيئة التشغيل اليدوي للبيانات، ولكن الاختلاف سيكون في طريقة استخدام وتنفيذ هذه المكونات والإجراءات [١].

ثانيا : تأثير تكنولوجيا المعلومات علي الرقابة الداخلية .

أدي استخدام تكنولوجيا المعلومات إلي تطوير الرقابة الداخلية وذلك من خلال إضافة إجراءات رقابية جديدة يؤديها الكمبيوتر بدلا من العناصر الرقابية اليدوية المليئة بالأخطاء، مما ساعد علي تقليل الأخطاء البشرية التي تحدث أثناء تشغيل العمليات اليدوية. ولذلك تتضح مميزات تأثير تكنولوجيا المعلومات علي الرقابة الداخلية في الآتي :

أ- إحلال العناصر الرقابية الإلكترونية محل العناصر الرقابية اليدوية [٢].

ب- توفير المعلومات ذات الجودة العالية [٣].

إلا أنه يوجد تحفظات علي استخدام تكنولوجيا المعلومات منها ظهور مخاطر جديدة متعلقة بأنظمة تكنولوجيا المعلومات يمكن أن تؤدي إلي خسائر جوهرية إذا تم تجاهلها. هذه المخاطر تتمثل في : -

- مخاطر المكونات المادية والبيانات ،
- اختفاء مسار المراجعة ،

---

[١] - أ.د / أحمد حسين علي حسين " دليلك في : تحليل وتصميم النظم " ،الدار الجامعية – الإسكندرية ، سنة ٢٠٠٦ ، ص٣٤٦ .

[2] - Alvin A. Arens , Randal J. Elder , Mark S. Beasley ," Auditing and Assurance Services ,12th Edition ", New Jersey , Prentice Hall , 2008, P 372 .

[٣] - د / ثناء علي القباني ،" مراجعة نظم تشغيل البيانات الكترونيا "، بدون ناشر، كلية التجارة – جامعة المنوفية، سنة ٢٠٠٨ ، ص ١٧٨ .

- الحاجة إلي خبرة وفصل المهام في تكنولوجيا المعلومات[١] .

ثالثا : تأثير نظام الرقابة الداخلية علي تكنولوجيا المعلومات[٢].

إن نظام الرقابة الداخلية يؤثر علي تكنولوجيا المعلومات في ثلاث مستويات هي :-

الإدارة العليا : تضع أهداف ، و تؤسس السياسات ، وتتخذ القرارات لتنفيذ الاستراتيجية وتوجه بيئة رقابة تكنولوجيا المعلومات لتحقيق أهداف المنشأة .

عمليات المنشأة : أغلب عمليات المنشأة الآن تكون مميكنة وتدمج مع أنظمة تطبيق تكنولوجيا المعلومات ، مما نتج عنه ميكنة كثير من عناصر الرقابة الخاصة بالعمليات ، وتعرف بعناصر رقابة التطبيق ، والتي تتطلب من وظيفة تكنولوجيا المعلومات أن تدعم تصميمها وتطويرها .

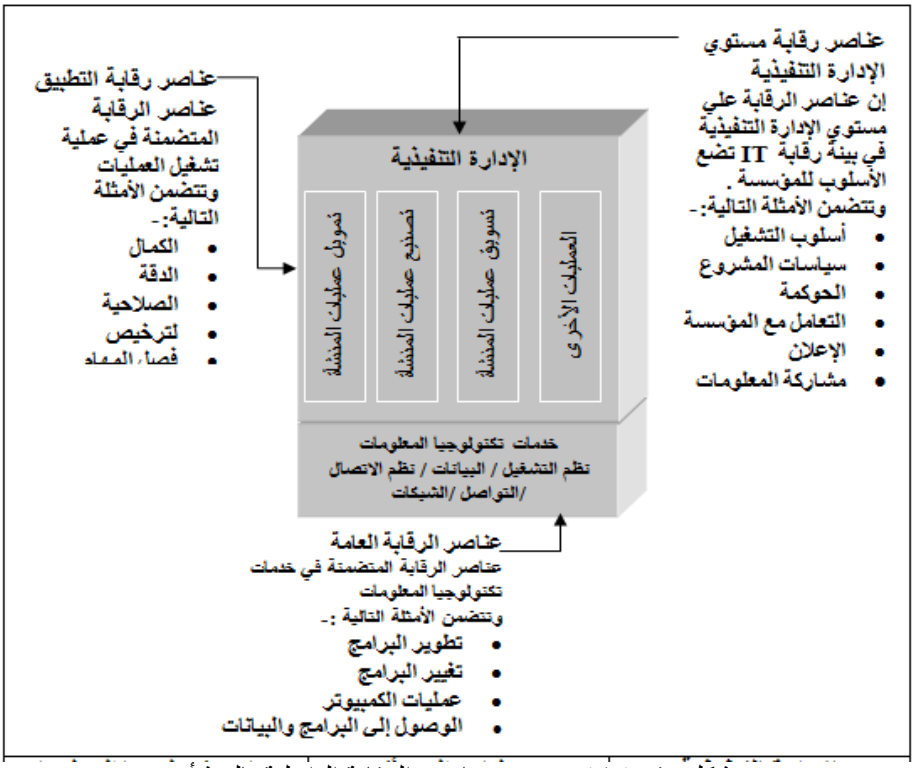
خدمات تكنولوجيا المعلومات : لدعم عمليات المنشأة توفر تكنولوجيا المعلومات خدماتها ، في شكل خدمة مشتركة لعمليات للمنشأة. وذلك لأن العديد من عمليات التطوير والتشغيل الخاصة بتكنولوجيا المعلومات تتوفر للمنشأة ككل، ومعظم البنية التحتية لتكنولوجيا المعلومات متوفرة كخدمة عامة (مثل شبكات المعلومات، قواعد البيانات وأنظمة التشغيل والتخزين). وتعرف عناصر الرقابة المطبقة علي كل أنشطة خدمة تكنولوجيا المعلومات باسم عناصر الرقابة العامة لتكنولوجيا المعلومات. ويوضح الشكل (١) كيف يتم تضمين عناصر الرقابة داخل كل مكون من مكونات المنشأة .

---

[1] - Alvin A. Arens , Randal J. Elder , Mark S. Beasley , 2008 , Op .Cit , p 372- 374 .

[2] - IT Governance Institute ,"COPIT 4.1 Excerpt - Executive Summary Framework ", IT Governance Institute, USA , 2007 , P 15 . http://www.ITgi.org

- IT Governance Institute, "IT Control Objectives for Sarbanes- Oxley", IT Governance Institute , 2004 , P20.



شكل رقم (١) يعرض عناصر الرقابة الداخلية بالمنشأة

المصدر:

IT Governance Institute," IT Control Objectives For Sarbanes-Oxley ", IT Governance Institute ,USA , 2004, P 20.

ومن استعراض المفاهيم الموجود بالشكل رقم (١) ، خلص الباحث إلي أن :-

١- الإدارة العليا هي المسئولة عن وضع كل من نظم الرقابة الداخلية ، ونظم الحوكمة لضمان تحقيق أهداف المنشأة .

٢- عناصر الرقابة العامة هي عناصر الرقابة المتضمنة في عمليات وخدمات تكنولوجيا المعلومات، وتشتمل علي تطوير الأنظمة ، إدارة التغيير ، الأمن ، وعمليات الكمبيوتر . أما عناصر الرقابة علي التطبيق فهي عناصر الرقابة المتضمنة في تطبيقات عمليات التشغيل ، وتشتمل علي الكمال ، الدقة ، الصلاحية ، الترخيص وفصل المهام .

٣- عناصر الرقابة العامة هي مسئولية إدارة تكنولوجيا المعلومات أما عناصر الرقابة علي التطبيق فهي من البداية إلي النهاية مسئولية مشتركة بين الإدارات المستخدمة لخدمات تكنولوجيا المعلومات و إدارة تكنولوجيا المعلومات ولكن طبيعة المسئوليات تتغير . ويمكن توضيح مسئوليات

إدارة تكنولوجيا المعلومات والإدارات المستخدمة لخدمات تكنولوجيا المعلومات كما يلي [1]:-

١/٣ - الإدارات المستخدمة لخدمات تكنولوجيا المعلومات مسئولة بدقة عن:

١/١/٣- تحديد المتطلبات الوظيفية والرقابية.

٢/١/٣- استخدام الخدمات الأوتوماتيكية

٢/٣ - إدارة تكنولوجيا المعلومات مسئولة عن:

١/٢/٣- ميكنة وتنفيذ المتطلبات الرقابية والوظيفية للعمل.

٢/٢/٣- إنشاء عناصر رقابة لتحقيق والمحافظة علي التكامل لعناصر الرقابة علي التطبيق.

٤- علي المراجع سواء كان داخلي أو خارجي تقييم فعالية عناصر الرقابة الداخلية في بيئة التشغيل الالكتروني المتمثلة في عناصر الرقابة العامة و عناصر الرقابة علي التطبيق[2] .

رابعا:أهمية نظام الرقابة الداخلية في ظل التشغيل الإلكتروني للبيانات.

لقد تزايدت أهمية وجود نظام الرقابة الداخلية في ظل نظام تشغيل البيانات إلكترونيا و ذلك لعدة أسباب هي :-

١ - يتم معالجة و تخزين بيانات العمليات المحاسبية في صورة غير قابلة للقراءة ولذلك لا يمكن للفرد مراقبة هذه البيانات و التحقق من دقتها و موضوعتيها و التي كان يسهل إجرائها في ظل النظام اليدوي للمعلومات المحاسبية [3].

٢ - يتم معالجة قدر كبير من البيانات المحاسبية بواسطة الحاسب الآلي يفوق التي كانت تعالج يدويا مما يترتب عليه زيادة احتمال الوقوع في أخطاء .

٣ - تركيز عدد كبير من خطوات النظام المحاسبي في قسم أو إدارة واحدة يؤدي بالتالي إلي تلاشي خصائص الرقابة الداخلية التي تتعلق بفصل الوظائف بين أفراد وإدارات المؤسسة المختلفة [4] .

٤ - يصعب تتبع مسار المراجعة مما قد يترتب عليه قيام الموظفين غير الأمناء باختلاس مبالغ طائلة من المؤسسات التي يعملون بها [1].

---

[1] - IT Governance Institute ,"COPIT 4.1 Excerpt - Executive Summary Framework ", IT Governance Institute, USA , 2007 , P 17 . http://www.ITgi.org

[2] - Alvin A. Arens , Randal J. Elder , Mark S. Beasley , 2008, Op. Cit , pp 380 - 381.

[3] - ستيفن . أ . موسكو ف ، مرجع سبق ذكره ، ١٩٨٤ ، ص ٢٨٦ .

[4]- Jack E. Kiger & James H . Scheiner ," Auditing ", New Jersey , Houghton Mifflin Company , 1994 , P 392 .

٥ - انتشار أنواع جديدة من الجرائم والغش المالي في ظل نظم التشغيل الإلكتروني[٢].
٦ - المخاطر الخاصة بنظام الاتصال الفوري .
٧ - تواجد أنظمة التشغيل الإلكتروني في مكان واحد أو عدة أماكن محدودة .
٨ - أصبح استخدام النظم الإلكترونية شيئا أساسيا حيث أصبح من الصعب الاعتماد علي النظام اليدوي في تشغيل هذه البيانات.
٩ - الآثار السيئة الناتجة عن إصابة نظم التشغيل الإلكتروني بالفيروسات و التكلفة الناتجة عن نقص الكفاءة و الفعالية و تكلفة وقت الأفراد المستغرق في التعرف علي الفيروس و إزالته ، و كذلك التكلفة الناتجة عن فقد ثقة المستخدمين في النظام [٣] .
١٠ - مع استخدام الإنترنت في مجال التجارة الإلكترونية تزداد أيضا حالات الغش المالي معتمدة علي أن جميع إجراءات الصفقات تتم من خلال الحاسب الآلي[٤].
١١ - ينتج نظام التشغيل الإلكتروني معلومات كثيرة و متنوعة تساعد الإدارة علي الإشراف الأفضل علي المنشأة كما تساعد المراجع في عملية المراجعة .
١٢- تزايد الاعتماد علي التعاقد مع الجهات الخارجية في توفير خدمات تكنولوجيا المعلومات للمؤسسة[٥].
١٣- التطور التقني في مجال أنظمة الاتصالات والأجهزة والبرمجيات، والذي يمكن من معالجة المعاملات بسرعة أكبر.

---

[١] - (أ)- د/ أحمد حسين علي حسين " مشاكل الرقابة في أنظمة التشغيل الإلكتروني للبيانات و أثرها علي مسئوليات المراجع الخارجي " ، مجلة البحوث العلمية ، كلية التجارة ، جامعة الإسكندرية ، العدد الأول ، ١٩٨٩ ، ص ٣٤٥ .
(ب)- د/ السيد أحمد السقا ، وآخرون ، " الاتجاهات الحديثة في المراجعة المالية "، كلية التجارة – جامعة طنطا، ٢٠٠٥ ، ص ١٢٨ .
C- R . Weber ," EDP Auditing :Conceptual Foundations and Practice " , London: McGraw - Hill Book Company , 1988 , P. 13 .

[٢] -د/ سمير محمد الجزار " الغش المالي من خلال أنظمة المحاسبة الإلكترونية و حتمية تطوير أساليب المراجعة و الرقابة الداخلية " ، مجلة التجارة و التمويل ، كلية التجارة – جامعة طنطا ، العدد الثاني ، السنة الثانية ، ١٩٨٨ ، ص ١٥٨ .

[٣] - د / محمد سامي راضي ،" المراجعة المتقدمة "، بدون ناشر، طنطا: كلية التجارة – جامعة طنطا، سنة ١٩٩٩-٢٠٠٠،ص ١٤٨.

[٤] - طلعت عبد العظيم متولي " تأثيرات الإنترنت علي المحاسبة و دور المحاسب في مجال الإنترنت " ، " دراسة تطبيقية لاستطلاع واقع استخدام الإنترنت في البيئة المصرية " ، (مجلة التجارة و التمويل ، كلية التجارة ، جامعة طنطا ، العدد الأول ، ١٩٩٨) ، ص ١١ .

[4]- اللجنة العربية للرقابة المصرفية " إدارة المخاطر التشغيلية و كيفية احتساب المتطلبات الرأسمالية لها " ، صندوق النقد العربي ، أبو ظبي ، سنة ٢٠٠٤ ، ص ٧ .

١٤- تزايد إمكانيات حدوث عمليات الاحتيال المالي نتيجة غياب المعايير والمبادئ الفعالة التي يمكن الاستناد عليها للتحقق والتثبت من هوية العملاء والمتعاملين ، في إطار الطبيعة المفتوحة لشبكة الانترنت.
١٥- النقص في الأطر التشريعية والقانونية الواضحة والشفافة المنظمة للأنشطة والعمليات المصرفية الإلكترونية .
١٦- بروز قضايا انتهاك الخصوصية بشكل متزايد في العمليات المالية والمصرفية الإلكترونية ، في ضوء ما تتضمنه هذه العمليات من مراحل متعددة لتجميع وانتقال متكرر للمعلومات والبيانات .

خامسا : مقومات نظام الرقابة الداخلية في ظل التشغيل الإلكتروني للبيانات

ينص المعيار رقم (٣) من معايير المراجعة علي أن[١]" تتضمن الرقابة الداخلية علي التشغيل بالحاسب الإلكتروني - التي تساعد علي تحقيق الأهداف العامة للرقابة الداخلية - إجراءات يدوية و إجراءات مصممة في برامج الحاسب الإلكتروني وتشمل هذه الإجراءات اليدوية و إجراءات رقابة الحاسب الإلكتروني الرقابة العامة التي تؤثر في بيئة التشغيل الإلكتروني للبيانات والرقابة الخاصة على التطبيقات المحاسبية".
و بالتالي فإنه يتم تصنيف عناصر الرقابة في نظم تشغيل البيانات إلكترونيا إلي[٢]:-

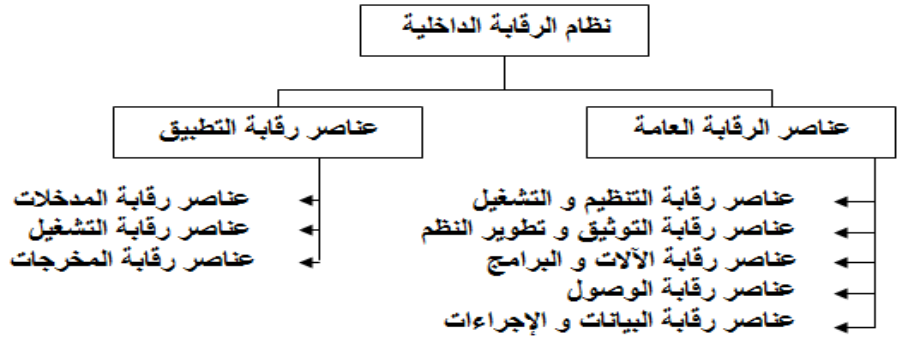
- عناصر الرقابة العامة General Controls

---

١ - المعهد المصري للمحاسبين و المراجعين - معايير المراجعة،(القاهرة ، بدون سنة نشر)، ص ١٦٦ .

٢- لمزيد من التفاصيل يمكن الرجوع الي :
* د/ ثناء القباني " الرقابة المحاسبية الداخلية في النظامين اليدوي و الإلكتروني " (دار الكتاب الجامعي ، الإسكندرية ، سنة ٢٠٠٣) ، ص ١٩٣ .
* د/ ثناء القباني " دراسات في المراجعة – برامج عملية المراجعة – مراجعة مجالات بيئة تشغيل البيانات الكترونيا - مراجعة التجارة الالكترونية "، بدون ناشر ، كلية التجارة – جامعة المنوفية ٢٠٠٨/ ٢٠٠٩ ، ص ٢٥٥ – ٣٣٣ .
* د/ محمد علي حماد ، " صوب هيكل رقابة داخلية فعال مع تطوير دور المراجع الداخلي والمراجع الخارجي وذلك في ظل النظم الالكترونية " (المجلة المصرية للدراسات التجارية ، كلية التجارة ، جامعة المنصورة – المجلد التاسع عشر ، العدد الرابع ١٩٩٥) ، ص ١٤- ٢٩ .
- Jack E . Kiger & James H. Scheiner ، op، cit، pp. 394 – 404 .
- D.H. Taylor and W.G.،Glezen ، " Auditing Integrated Concepts and Procedures " ، (N.Y. ، John Wiley & Sons ، Inc. ، 1991) ،pp. 405 – 418 .
- Walter G. Kell and William C. Boynton ، " Modern Auditing " (New York : John Wiley & Sons ، Inc. ، 1992) pp. 440 – 444 .
* د/ محمد سامي راضي " المقومات الرقابية الملائمة في ظل التشغيل الإلكتروني للبيانات " (مجلة التجارة و التمويل ، مكتبة كلية التجارة ، جامعة طنطا ، العدد الثاني ، السنة الثامنة ١٩٨٨) ، ص ٩- ٣٦ .

- عناصر رقابة التطبيق Application Controls



العلاقة بين عناصر الرقابة العامة و عناصر رقابة التطبيق

عناصر الرقابة العامة تتعلق بكل مفاهيم وظيفة تكنولوجيا المعلومات شاملة إدارة وظائف تكنولوجيا المعلومات ،الفصل بين وظائف تكنولوجيا المعلومات، تطوير النظم، حيازة البرامج وصيانتها، الأمان الفعلي والأمان المباشر ضد أخطار الدخول إلي الآلات والبرامج والبيانات المتعلقة بها والنسخ البديلة ،وكذلك الاحتياط وتخطيط الطوارئ و مخاطر الرقابة علي الآلات. ويجب أن يقوم المراجع بتقييم عناصر الرقابة العامة للمؤسسة ككل أي كوحدة واحدة [١]. وهي رقابة مانعة في طبيعتها حيث يعني وجودها الوقاية من حدوث الأخطاء[٢].

أما عناصر رقابة التطبيق فتطبق عند تشغيل العمليات وهي رقابة مكتشفة ومصححة في طبيعتها .فهي مكتشفة لأنها تكشف الأخطاء بعد حدوثها ، ومصححة لأنها تتأكد من أن الأخطاء التي تم اكتشافها قد تم تصحيحها . وهي رقابة خاصة في طبيعتها لأنها تركز علي دورات العمليات (دورة الإيراد ، دورة الإنفاق ..... الخ) والنظم التطبيقية المشتركة في هذه الدورات . ويتمثل الهدف العام لرقابة التطبيق في التحقق من أن العمليات مصرح بها وأنه تم تسجيلها وتشغليها والتقرير عنها بالدقة المطلوبة [٣] . وعلي ذلك تتعلق عناصر رقابة التطبيق بتطبيقات معينة ولا تؤثر علي كل وظائف تكنولوجيا المعلومات . ولذا يجب تقييم عناصر رقابة التطبيق لكل مجال مراجعة (كل حساب أو مجموعة عمليات) يتأثر بالتطبيق والذي يقوم المراجع بالتخطيط لمراجعته بما يؤدي إلي تقليل الخطأ الرقابي المحتمل[٤]. حيث يتم تصميم عناصر الرقابة علي التطبيق لكل برنامج تطبيقي لمساعدة المؤسسة علي تحقيق أهداف مراجعة

---

[1] - Alvin A. Arens , Randal J. Elder , Mark S. Beasley , Op.Cit ,2008, p 374 .

[٢]- أ.د / أحمد حسين علي حسين ، " دليلك في : تحليل وتصميم النظم " ، مرجع سبق ذكره، ص٣٥٤ .

[٣]- نفس المرجع السابق ، ص ٣٦٦ .

[٤]- أ.د / ثناء علي القباني " مراجعة نظم تشغيل البيانات الكترونيا " ، ٢٠٠٨، مرجع سبق ذكره ، ص ١٨٣ .

العمليـات (الوجـود – الاكتمـال – الدقـة – التبويـب – التوقيـت – الترحيـل والتلخيص)، ورغم أن بعض عناصر الرقابة علي التطبيق تؤثر علـي واحد أو عدد قليل من أهداف مراجعة العمليات فإن معظم العناصر الرقابية تمنع أو تكتشف عدة أنواع من الأخطاء . ويمكن إتمام عناصر الرقابة علي التطبيق بواسطة الكمبيوتر أو بواسطة الأفراد . وتقسم عناصر الرقابة علي التطبيق إلي ثلاث مجموعات (عناصر رقابة المدخلات ، التشغيل و المخرجات) وتتشابه أهداف كل مجموعة مع الأخرى إلا أن إجراءات تحقيق هذه الأهداف تختلف[1].

ويجب ملاحظة أن عناصر رقابة التطبيق الأوتوماتيكية تحل محل عناصر الرقابة اليدوية. وتكون عناصر الرقابة العامة أكثر أهمية، حيث أن عناصر رقابة التطبيق تتواجد داخل البرامج لمنع واكتشاف العمليات الغير مصرح بها، وتؤكد علي الاكتمال والدقة والتفويض وصلاحية عمليات التشغيل. وعناصر الرقابة العامة تلزم لدعم التوظيف لعناصر رقابة التطبيق، وكلاهما يلزم للمساعدة في التأكيد علي التشغيل الدقيق والتكامل للمعلومات الناتجة والمستخدمة في الإدارة، والرقابة والتقرير عن المؤسسة.

و يجب أن يكون المراجع الداخلي علي علم بكل من الرقابة العامة ورقابة التطبيق، سواء كان استخدام المؤسسة لتكنولوجيا المعلومات بسيط أو معقد، ومعرفة الرقابة العامة تزيد من قدرة المراجع في تقييم والاعتماد علي رقابات التطبيق الفعالة لتقليل خطر الرقابة لأهداف المراجعة [٢].ولذا يجب علي المراجع أن يقوم بتقييم فاعلية عناصر الرقابة العامة قبل تقييم عناصر رقابة التطبيق، حيث أن عناصر الرقابة العامة لها تأثير قوي علي فاعلية عناصر رقابة التطبيق. فإذا كانت عناصر الرقابة العامة غير فعالة فإنه يوجد احتمال وجود أخطاء هامة في كل تطبيق محاسبي يعتمد علي الكمبيوتر، وذلك بغض النظر عن نوعية عناصر رقابة التطبيق. ومن ناحية أخري إذا توافرت عناصر الرقابة العامة يوجد احتمال كبير لزيادة الاعتماد علي عناصر رقابة التطبيق. ويوضح الشكل رقم (٢) العلاقة بين عناصر الرقابة العامة و عناصر رقابة التطبيق.

و تعتبر المراجعة الداخلية من العناصر الهامة في نظام الرقابة الداخلية فهي تعمل علي تطويره وتحسينه وزيادة فعاليته وكفاءته، حيث أكدت العديد من الدراسات والإصدارات المهنية علي أنه يجب أن يكون للمراجعة الداخلية دور

---

[1] - Alvin A. Arens , Randal J. Elder , Mark S. Beasley , Op.Cit ,2008, p 378 .

[2] - The same previous reference,p 380 .

في إعداد تقرير الإدارة عن فعالية نظام الرقابة الداخلية بالمؤسسة وذلك عن طريق متابعة تشغيل وتقييم نظام الرقابة الداخلية وإخطار الإدارة بنقاط الضعف والقوة الموجودة فيه[1]. حيث أصدر مجمع المراجعين الداخليين بالولايات المتحدة IIA في عام ١٩٩٤ نشرة مقترحة لمعايير المراجعة الداخلية بعنوان التقرير عن نظم الرقابة الداخلية ككل Reporting on Overall System of Internal Control حيث تضمنت تلك النشرة نموذج مقترح لتقرير إدارة المراجعة الداخلية عن فعالية نظام الرقابة الداخلية ، وفي نفس العام صدر تقرير لجنة COCO في كندا و أيضا تقرير لجنة Rutteman بهذا الخصوص . و طالب تقرير لجنة COSO بالولايات المتحدة عام ١٩٩٢، وتقرير لجنة Cadbury في نفس العام ، ولجنة Hampel في عام ١٩٩٨، ولجنة Turnbull في عام ١٩٩٩ في المملكة المتحدة وذلك بضرورة إعداد تقرير عن فعالية نظم الرقابة الداخلية بمعرفة الإدارة . ولكن هذه المتطلبات كانت تمثل مقترحات أو توصيات ولكنها غير ملزمة . وجاء قانون Sarbanes-Oxley ملزما عام ٢٠٠٢ في المقطع 404-A حيث ألزم القانون إدارة كل شركة مساهمة بإصدار تقرير ضمن التقرير المالي السنوي يؤكد مسئولية مجلس الإدارة عن وجود نظام للرقابة الداخلية وتنفيذه بفعالية [2].

كما أوضحت معايير الأداء المهني للمراجعة الداخلية دورها فيما يتعلق بنظم الرقابة الداخلية في المعيار رقم 2130 علي أنه " يجب علي نشاط المراجعة الداخلية مساعدة المنشأة في الحفاظ علي نظم رقابية فعالة عن طريق تقييم فعاليتها وكفاءتها وضمان التطوير والتحسين المستمر لها[3]".

---

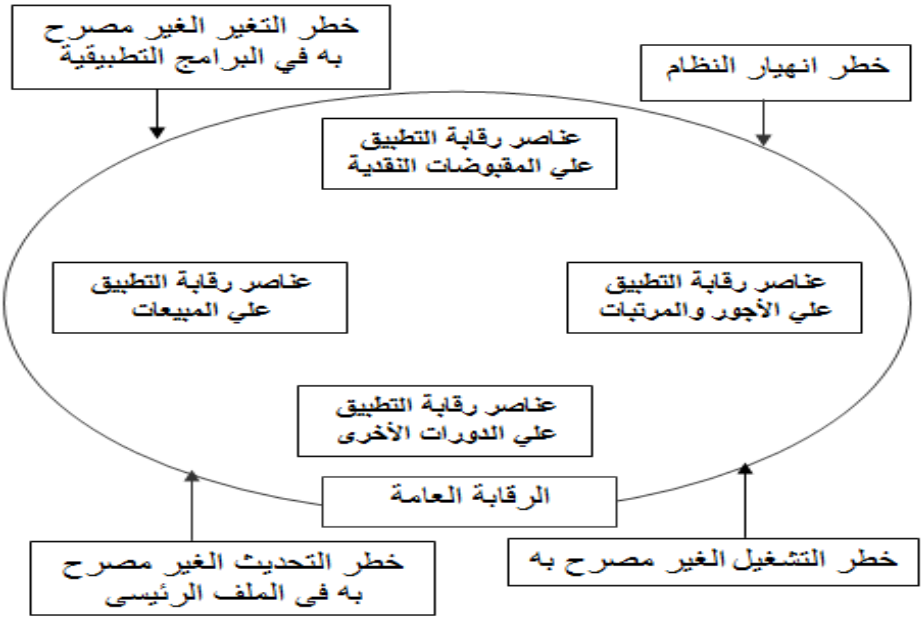
[1] - د/ نصر عبد الوهاب، د/ شحاتة السيد شحاتة،" الرقابة والمراجعة الداخلية الحديثة في بيئة المعلومات وعولمة أسواق المال " ، الإسكندرية : الدار الجامعية ، ٢٠٠٦ ، ص ص ١٠٣- ١٠٤ .

[2] - The Institute Of Internal Auditors, " Sarbanes – Oxley Section 404 : A Guide for Management by Internal Controls Practitioners ", AII, 2nd Edition , January 2008 ,PP 18 – 21 .www.theiia.org .

- Henning Hagerman , William Kinney , Karlheinz Kuting , Claus-Peter Weber ," Internal Audit Handbook Management with the SAP-® Audit Roadmap ", German : Acid-free paper ,2008 ,P 570.

- Rosslin John Robles , and others , " SOX and Its effects on IT security Governance ", Op. Cit ,P 83 .

[3] - The Institute Of Internal Auditors (IIA) , " International Standards for the Professional Practice of Internal Auditing " , USA , Florida , 2010, P12 .



الشكل رقم (٢) يوضح العلاقة بين عناصر الرقابة العامة و عناصر رقابة التطبيق

المصدر :

Alvin A. Arens , Randal J. Elder , Mark S. Beasley ," Auditing and Assurance Services ,12th Edition ", New Jersey ,Prentice Hall ,2008 , P 375 .

سادسا :- مخاطر تكنولوجيا المعلومات :

أ- مفهوم مخاطر تكنولوجيا المعلومات

يمكن تعريف مخاطر تكنولوجيا المعلومات [1] علي أنها " مجموعة المخاطر المرتبطة باستخدام ، وحيازة ، وتضمين ، وتأثير وتبني تكنولوجيا المعلومات داخل المنشأة . وهي تتضمن كل من التكرار والتأثير الغير مؤكدان ، و تخلق تحديات لتحقيق الغايات والأهداف الاستراتيجية وكذلك عدم التأكد في متابعة الفرص " . ويجب ملاحظة أن مخاطر تكنولوجيا المعلومات توجد دائما ، سواء تم اكتشافها أو لم يتم ذلك من خلال إدارة المنشأة ، وعلي ذلك نجد أن مديري تكنولوجيا المعلومات يحتاجون إلي تأسيس سياسات وإجراءات سليمة لرقابة المخاطر الرئيسية المتعلقة بعمليات تكنولوجيا المعلومات.

[1] -IT Governance Institute ,"Enterprise Risk : Identify, Govern and Manage IT Risk – The Risk IT Framework " , IT Governance Institute ,USA , 2009 , p 11 .

ب- أنواع مخاطر تكنولوجيا المعلومات

تباينت وتنوعت الآراء حول تصنيف مخاطر تكنولوجيا المعلومات حيث يوجد عدة تصنيفات لها . وفيما يلي عرض لأهم هذه التصنيفات :-

التصنيف الأول : [1] يقوم بتصنيف مخاطر تكنولوجيا المعلومات إلي :

١- مخاطر الاستثمار أو الإنفاق Investment or Expense risk
٢- مخاطر الوصول أو الأمن Access or Security risk
٣- مخاطر السلامة (التكامل) Integrity risk
٤- مخاطر الملاءمة Relevance risk
٥- مخاطر الإتاحة Availability risk
٦- مخاطر البنية التحتية Infrastructure risk
٧- مخاطر ملكية المشروع Project ownership risk

التصنيف الثاني : قامت لجنة التكنولوجيا المنبثقة من الاتحاد الدولي للمحاسبين IFAC بتصنيف مخاطر نظم تكنولوجيا المعلومات إلي ثلاث أنواع رئيسية من المخاطر هي[٢]:-

١- مخاطر البنية التحتية لنظم تكنولوجيا المعلومات .
٢- مخاطر تطبيق تكنولوجيا المعلومات .
٣- مخاطر تكنولوجيا المعلومات الخاصة بأعمال المنشأة .

التصنيف الثالث : [٣] يقوم بتصنيف مخاطر تكنولوجيا المعلومات إلي :

١- مخاطر تكنولوجيا المعلومات علي مستوي المنشأة.
٢- مخاطر تكنولوجيا المعلومات علي مستوي العملية التشغيلية (المخاطر العامة لتكنولوجيا المعلومات).
٣- المخاطر الخاصة بتكنولوجيا المعلومات (مخاطر تطبيقات وخدمات تكنولوجيا المعلومات)

ويعتبر التصنيف الأول هو التصنيف الذي يلائم فكرة الدراسة .

---

[1]- The National Computing Centre ,"IT Governance : Developing a successful governance strategy", National Computing Centre (NCC) , 2005 , p 29 .

[٢] - د/ محمد محمد إبراهيم منصور ، " تأثير التجارة الالكترونية علي تصميم نظم المعلومات المحاسبية – إطار مقترح - " ، مؤتمر التجارة الالكترونية الآفاق والتحديات ، كلية التجارة جامعة الإسكندرية، المجلد الأول ، الإسكندرية ٢٥- ٢٧ يوليو٢٠٠٢، ص ١٧٢-١٧٣

[3] - Mario Spremic ," IT Governance and IT Risk Management for Supporting ' Always-on ' Enterprise Information Systems" , IGI Global , 2010, p 8 .

سابعا : أثر جائحة كورونا علي تطبيق عناصر الرقابة الداخلية في بيئة التشغيل الإلكتروني للبيانات :

أدي انتشار فيروس كورونا إلي اصابة أفراد المجتمع مما أدي إلي أن تلجأ الحكومات والمؤسسات إلي اتباع بعض الإجراءات الاحترازية وذلك للحد من انتشار الفيروس منها :

أ- تخفيف العمالة :

قد يؤدي تخفيف العمالة في إدارات تكنولوجيا المعلومات إلي التخلي عن مبدأ الفصل في المهام ، ومفهوم العزل في المعرفة وبصفة خاصة مع المشغلين ، حيث سيتم منح المشغلين صلاحيات أكثر للاطلاع علي البيانات والمعلومات الخاصة بالتشغيل و البرامج المستخدمة لتسير العمل . مما يؤدي إلي ضعف نظم الرقابة الداخلية و قد يؤدي ذلك إلي زيادة احتمالات اختراق الأنظمة من الداخل أي زيادة التهديدات والمخاطر الداخلية . حيث تعد المخاطر الداخلية من أكثر المخاطر تهديد لنظم المعلومات ؛ اذ أنها تعد في الأساس مشكلة أفراد علي علم تام بالنظام ونقاط القوة والضعف به مما يعرض المؤسسات لبعض الأضرار المحتملة مثل الخسائر في الإيرادات ، سرقة أموال العملاء أو مخاطر السمعة ، أو سرقة الملكية الفكرية وغيرها من المخاطر.

ب- الأغلاق التام :

لجأت بعض الحكومات بسبب تفشي فيروس كورونا بشكل سريع ومتنامي وعجز المنظمات الصحية لهذه الدول إلي اتباع سياسة الأغلاق التام والكامل. مما دفع بعض الشركات والمؤسسات إلي تكليف موظفيها بالعمل من المنازل واستخدام أجهزة الحاسب الشخصية لكل منهم في القيام بأعمالهم الخاصة بالشركات والمؤسسات . وأدي هذا إلي عدم استخدام البنية التحتية المؤمنة للمؤسسات في عملية الدخول علي البيانات والمعلومات واستخدام الأجهزة الشخصية للعاملين غير المؤمنة مما يسهل علي المتلصصين من وجود ثغرات أمنية للدخول علي الأجهزة و شبكات الاتصال و البرامج ،والعمليات الخاصة بالمؤسسات . وقد يؤدي استخدام العاملين الأجهزة الشخصية الغير مؤمنة تأمين كافي إلي وقوع بعض المخاطر وذلك بسبب سهولة اختراق هذه الأجهزة الشخصية من المتلصصين منها :

- مخاطر الوصول أو الأمن Access or Security risk : هي خطر تسرب المعلومات الضرورية و الحساسة لغير المخولين لذلك .
- مخاطر السلامة (الكمال) Integrity risk : و هي خطر أن البيانات لا يمكن الاعتماد عليها لأنها غير مرخصة أو غير كاملة أو غير دقيقة .

- مخاطر الملاءمة Relevance risk: و هي المخاطر المرتبطة بعدم وصول المعلومات السليمة (المناسبة) للشخص المناسب (أو العملية أو النظم) في الوقت المناسب حتى تسمح باتخاذ الإجراء المناسب.
- مخاطر التوافرAvailability risk : و هي مخاطر فقد الخدمة .

فمن الواضح أن الطبيعة المفتوحة للمعاملات الإلكترونية من خلال شبكات الاتصال ، خلقت قضايا أمنية لإدارات المؤسسات المالية تتعلق بالسرية و سلامة المعلومات و التحكم في الدخول إلي الأنظمة و الشبكات و التأكد من هوية المستخدمين، بالإضافة إلي الاحتفاظ بسجلات للمعاملات. و مما لا شك فيه أن الضعف أو الخلل في التعامل مع هذه القضايا قد يقود إلي مخاطر إضافية لإدارة المؤسسات المالية كالمخاطر القانونية و مخاطر السمعة. و يتعين علي هذه المؤسسات مراعاة عدد من المبادئ في هذا الخصوص:

- إتباع سياسات و إجراءات تحقق تأمين الاتصالات من و إلي النظم لمنع أو الحد من اختراق غير المرخص لهم للنظم أو إساءة استخدامها.
- الرقابة علي دخول النظم و تحديد شخصية المستخدمين.
- حماية النظم من احتمالات القيام بممارسات غير مرخص بها من قبل العاملين بالمؤسسة السابقين أو الجدد أو المؤقتين.
- التأكد من وجود نظم تحويل سليمة للدخول علي الأنظمة الإلكترونية الخاصة بشبكة الإنترنت.
- التأكد من وجود الإجراءات المناسبة لحماية المعلومات المتعلقة بالمعاملات الإلكترونية و السجلات و المعلومات، و المحافظة علي سرية هذه المعلومات أثناء انتقالها أو تخزينها.
- وجود آليات و قواعد واضحة لتدقيق جميع المعاملات الإلكترونية.
- كما يتعين علي المؤسسات معالجة المخاطر الأمنية التي قد تنشأ من شبكاتها الداخلية .

بالإضافة إلي التأكد من كفاءة الإجراءات الأمنية و سلامة البيانات، فإن انتظام توفير الخدمات المصرفية الإلكترونية علي مدار الساعة يمثل عنصرا هاما من مكونات إدارة و توفير هذه الخدمات، الأمر الذي تعززه متطلبات المنافسة من جهة و الحاجة إلي الحد من مخاطر السمعة التي قد تنشأ من عدم انتظام الخدمة من جهة أخري. و لذلك يتعين علي المؤسسات المالية ما يلي:-

- أن تحدد الآليات البديلة لاستئناف الخدمة في حال أي توقف. و يجب توجيه اهتمام خاص للقدرة علي استرجاع السجلات الإلكترونية و المادية الضرورية لاستئناف الأعمال.
- أن تقوم بمراجعات دورية لخطط الطوارئ و مواصلة الأعمال حتى تكون متسقة مع العمليات الجارية للبنك و خططه الاستراتيجية. و يجب علاوة علي ذلك إخضاع الخطط لاختبارات دورية لضمان قدرة البنك علي تنفيذها في حال التعرض لتوقف خطير في الأعمال[١] .
- كما يتعين علي البنوك إيجاد بدائل في حالة الاعتماد علي المورد الخارجي في توفير هذه الخدمات.
- كما يجب الأخذ في الاعتبار حدوث أعطال ما في شبكة الإنترنت و العمل علي تبني خطط للطوارئ في هذه الحالة.
- قد يكون من المفيد التعاقد مع أحد بيوت الخبرة لاكتشاف الخلل في الأنظمة و بصورة دورية و ذلك للحد من الهجمات التي قد تساهم في تعطيل انتظام الخدمة.

المحور الثالث : ماهية أمن المعلومات .

يتناول هذا المحور العناصر التالية :

أولا : مفهوم أمن المعلومات .

ثانيا : التهديدات التي تتعرض لها المعلومات وأنظمتها .

ثالثا : الهجمات الإلكترونية وأنواعها . كما يلي :

أولا : مفهوم أمن المعلومات :

يمكن تعريف أمن المعلومات علي أنه " العلم الذي يعمل علي توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية " . كما يمكن تعريفه علي أنه " المفاهيم والتقنيات والتدابير التقنية والإدارية المستخدمة لحماية أصول المعلومات من الوصول غير المسموح به عمدا أو سهوا أو حيازتها أو الإضرار بها ، أو كشفها أو التلاعب بها ، أو تعديلها أو فقدها أو إساءة استخدامها " [٢] .

ومع تطور تكنولوجيا المعلومات والاتصالات وخاصة الانترنت بدأ يظهر مفهوم أمن المعلومات بشكل ضروري وملح وذلك للحفاظ علي سرية البيانات

---

[١] - اللجنة العربية للرقابة المصرفية " إدارة المخاطر التشغيلية و كيفية احتساب المتطلبات الرأسمالية لها " ، مرجع سبق ذكره ، ص ٢٠ .

[2] - McDaniel, George(1994), "IBM Dictionary of Computing", McGraw-Hill, Inc, New York, 1994.

والمعلومات المتداولة علي الانترنت وعلي ذلك تم وضع التعريف التالي لأمن المعلومات علي أنه " عبارة عن مجموعة الإجراءات الخاصة بحماية نظم المعلومات وتأمين المعلومات المتداولة عبر الإنترنت من الوصول أو الاستخدام غير المصرح به أو الكشف عنها أو تعطيلها أو تعديلها أو إتلافها ". كما قامت لجنة الأمن القومي لنظم المعلومات The Committee on National Security Systems بتعريف أمن المعلومات علي أنه " حماية المعلومات وعناصرها الهامة بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزنها وترسلها "[1] . ويعتبر هذا التعريف هو التعريف الأنسب لأنه يشمل المعلومات بكافة أشكالها وعناصرها ويشتمل علي الأجهزة والبرامج التي تخزن وتعالج وترسل هذه المعلومات . وبهذا يتسع مفهوم أمن المعلومات ليشمل المحاور الآتية :

- حماية المعلومات من الضرر بكافة أشكاله ، من حيث المصدر سواء أشخاص (الهاكرز) أم برامج (الفيروسات) أو كان سهوا أو متعمد .
- حماية المعلومات من الوصول غير المصرح به ، او السرقة ، أو الالتقاط ، أو التغيير ، أو إعادة التوجيه ، أو سوء الاستخدام .
- حماية قدرة المنشأة علي الاستمرار وأداء أعمالها علي أحسن وجه .
- تمكين أنظمة تكنولوجيا المعلومات والبرامج التطبيقية لدي المنشأة من العمل بشكل آمن .

ومن أجل توفير بيئة آمنة يشترط أن يكون هناك مزيج من العناصر الأساسية لأمن المعلومات . كما يجب أن يتم استخدام مجموعة من الوسائل وذلك للحفاظ علي البيانات والمعلومات الخاصة بالشركات والمؤسسات المختلفة . وتقوم هذه الوسائل في معظمها علي استخدام نظام التعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته وهذه الوسائل تهدف إلي ضمان استخدام النظام أو الشبكة من الشخص المخول له بالاستخدام ، وتضم هذه الطرق كلمات السر بأنواعها ، والبطاقات الذكية المستخدمة للتعريف ، وسائل التعريف البيولوجية والتي تعتمد علي سمات معينة في الشخص المستخدم المصرح له باستخدام البيانات والمعلومات ، ويمكن أن نضم الي هذه الطرق ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفوذ .

---

[1] -A- The Committee on National Security Systems: http://www.cnss.gov
B - Withman, M. and Mattord, H.(2005), "Principles of Information Security", Second Edition, Thomson Course Technology, 2005, p 34.

ثانيا : التهديدات التي تتعرض لها المعلومات وأنظمتها .

هناك تهديدات كثيرة تحيط بأنظمة المعلومات شأنها في ذلك شأن أي نظام مفتوح يمكن الوصول إليه بأكثر من طريقة ، ومن قبل أشخاص مختلفين سواء من داخل المنشأة أو خارجها ، وفي أوقات مختلفة . وتتعدد هذه التهديدات وتتنوع بتنوع هياكل أنظمة المعلومات ونقاط الضعف فيها (الثغرات) ويمكن تقسيم تهديدات أمن المعلومات إلي ثلاث فئات رئيسية تحتوي كل فئة علي عدد كبير من التهديدات والتي تشترك في خصائص عامة واحدة ، وهذه الفئات هي كما بالجدول رقم (١):

جدول رقم (١) يوضح أنواع التهديدات لأمن المعلومات

التهديدات	التعريف	مصادر التهديدات
١- تهديدات فنية	تتمثل في التهديدات الناجمة عن القصور والأخطاء الفنية في مختلف أنظمة أمن المعلومات والتي يغلب عليها الطابع الفني بدون أي تدخل بشري .	- تهديدات عيوب التصميم والتشغيل : وتتمثل في عيوب التصميم في الأجهزة والبرامج والشبكات وكذلك عيوب التشغيل التي قد تؤدي الي النفاذ إلي المعلومات بطريقة غير شرعية . - تهديد تشتت المعلومات : يؤدي تشتت المعلومات إلي تطبيق أنظمة أمن معلومات متعددة بتعدد أماكن المعلومات وهو ما قد يؤدي إلي وجود ولو ثغرة يمكن من خلاله النفاذ إلي كامل منظومة المعلومات للمنشأة
وهنا تظهر أهمية التصميم الجيد للبنية التحتية لتكنولوجيا المعلومات وأمن المعلومات ، وأيضا أهمية التصميم الجيد لنظم للرقابة الداخلية للمؤسسة مثل : - أنظمة حماية الشبكات والتوصيلات . - أنظمة حماية البنية التحتية . - أنظمة حماية نظم التشغيل . - أنظمة حماية البرامج والتطبيقات . - أنظمة حماية قواعد البيانات . - أنظمة حماية الوصول أو الدخول غير المصرح للبيانات والمعلومات .		
٢- تهديدات بشرية	التهديدات الناجمة عن العنصر البشري سواء عمدا أو عن طريق الخطأ في الوصول غير المصرح	وتتعد مصادر التهديدات البشرية لنظم المعلومات في الآتي : - المستخدم الشرعي الفاسد

	به إلي المعلومات وذلك لإتلافها أو تسريبها أو الحاق الضرر بالعملاء أو استخدامها بطريقة غير أخلاقية .	- موظف المنشأة الفاسد - المستخدم الشرعي و موظف المنشأة غير الواعيين بالمخاطر الأمنية - الشركات المنافسة . - الهاكرز . - المنظمات الإرهابية. - موردوا الأجهزة والبرامج . - الدعم الفني الخارجي .

وللحد من هذه التهديدات يجب توفير مجموعة من الضوابط والإجراءات والتحقق من الالتزام بها وبصفة خاصة في إدارات تكنولوجيا المعلومات والتي تتحكم في أنظمة المعلومات الخاصة بالشركات والمؤسسات المختلفة مثل :

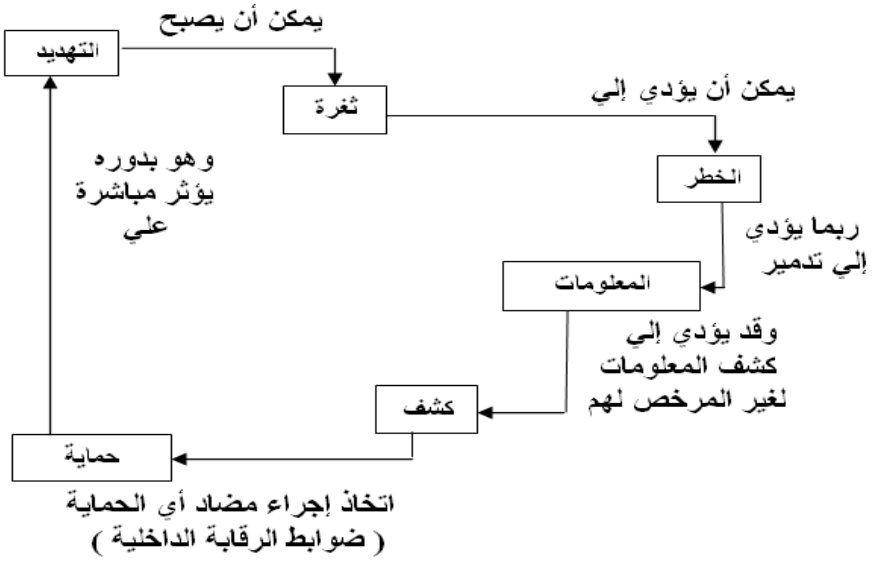
- ❖ الدخول للشركات والمؤسسات باستخدام البطاقات الخاصة بكل منهم .
- ❖ وضع حساسات Sensors حريق قرب أجهزة تخزين البيانات .
- ❖ استخدام الأجهزة الخاصة بالشركات والمؤسسات المختلفة من قبل الموظفين في حالة استخدام الانترنت ، وعدم استخدام أجهزة أخري مثل الأجهزة الشخصية مثل Laptop .
- ❖ تحديد الوظائف المختلفة داخل إدارة تكنولوجيا المعلومات والفصل بينها وذلك تحقيقا لمبدأ الفصل بين المسئوليات وتقسيم العمل .
- ❖ استخدام مفهوم العزل في المعرفة وبصفة خاصة مع المشغلين ، حيث أن وظيفتهم تتيح لهم فرصة الاطلاع علي البيانات والمعلومات الخاصة بالتشغيل وعلي البرامج المستخدمة ، لذا فمن المفضل ألا يكون لهؤلاء المشغلين معرفة بكيفية إعداد البرامج والقيام بإجراء التعديلات عليها، حيث يجب عدم تمكين أي فرد من التحكم في النظام بأكمله أو في الأنظمة الفرعية المكونة له لأن ذلك يزيد من احتمالات اختراق الأنظمة [١] .
- ❖ تقييد الوصول للبيانات والمعلومات من خلال تطبيق [٢] :
  - o التصريح بالاستخدام : مثل تخصيص شفرات للأشخاص المسموح لهم لكي يستخدموها عند الحاجة إلي الوصول للبيانات .
  - o وضع أجهزة للتحقق من بصمة الشخص علي أجهزة البيانات المهمة .
  - o تقييد الاستخدام : مثل ضبط الوحدات الطرفية بحيث تتوقف بعد عدد معين

[١] - د/ محمد سامي راضي " المراجعة المتقدمة " ، كلية التجارة ، جامعة طنطا ، ، بدون ناشر ٢٠٠٠، ص ١٥٠ – ١٥٨ .

[٢] - د/ أحمد حسين علي حسين ، " دليلك في : تحليل وتصميم النظم " ، اسكندرية – الدار الجامعية ، ٢٠٠٦ ، ص٣٥٩-٣٦٠ .

	من محاولات الوصول من شخص غير مرخص له بالدخول . ○ التشفير :بحيث لا يتم نقل البيانات الحساسة والهامة جدا في صورتها العادية بل يتم نقلها في صورة شفرات أو رموز لا يعرفها إلا مستخدمها المصرح له بذلك . ○ التدمير : ويقصد به التخلص كلية من البيانات الحساسة جدا بعد استخدامها إما بحرقها إذا كانت مطبوعة أو محوها إذا كانت علي وحدات التخزين . ❖ مسح كلمة السر الخاصة بالموظف المنتهي عقده فورا . ❖ الفصل في الأدوار والمسئوليات بين إدارة تكنولوجيا المعلومات والإدارات الأخرى المستفيدة من خدمات تكنولوجيا المعلومات . ❖ وجود نظام جيد لتوثيق البرامج الجديدة وأي تعديلات تجري عليها.	
٣- تهديدات طبيعية	تكون بسبب كارثة طبيعية ليس للإنسان أو التجهيزات الفنية دخل في حدوثها .	- الزلازل . - البراكين . - الصواعق ، والحرائق وغيرها

ويعرض الشكل رقم (٣) كيفية استغلال التهديد وذلك للنفاذ الي المعلومات بطريقة غير مصرح بها للعمل علي تدميرها أو استخدامها استخدامات غير أخلاقية ، وايضا وضع نظام للرقابة الداخلية يشمل إجراءات الحماية من هذه التهديدات



الشكل رقم (٣)
يعرض تطور التهديدات التي تتعرض لها نظم المعلومات بالمنشأة

ثالثا : الهجمات الإلكترونية وأنواعها [1]:

ويتناول هذا العنصر كل من :

- تصنيف مرتكبي الجرائم الإلكترونية علي أساس الغرض من الاعتداء.
- تصنيف الهجمات الإلكترونية علي أساس طرق أو كيفية الوصول إلي الأنظمة . كما يلي :

تصنيف مرتكبي الجرائم الإلكترونية علي أساس الغرض من الاعتداء:

تشكل المعلومات في الآونة الأخيرة أحد أهم عوامل نجاح أو فشل المؤسسات المختلفة . إلا انها يحيط بها عدد من المخاطر أو الأعداء يجب حمايتها منهم ، وكل منهم لديه طرق واساليب مختلفة يستخدمها للوصول اليها ، وبمجرد النفاذ الي المعلومات ، فإنه يمكن نسخ أو تعديل أو حذف أو اساءة استخدامها ، أو الحاق الضرر بها بأي شكل من الأشكال . ويمكن تصنيف مرتكبي الجرائم الإلكترونية علي أساس الغرض من الاعتداء علي أنظمة المعلومات الإلكترونية كما يلي :

١- المخترقون أو المتطفلون Hackers :

وهم أشخاص بارعين في استخدام الكمبيوتر وبرامجه ويكون لديهم فضول في فك الشفرات واقتحام حسابات الأخرين بطرق غير شرعية . ويكون غرضهم الأساسي هو محاولة التأكد من حرية المعلومات عن طريق جعل إمكانية الوصول لأجهزة الكمبيوتر والمعلومات عملية غير مقيدة ، وبذلك لا يقومون بالسرقة أو التخريب علي الإطلاق وإنما ينطلقون بدافع التحدي وإثبات الذات . وتتألف هذه الفئة أساسا من المراهقين والشباب العاطلين عن العمل [2].

٢- فئة الكراكرز Crackers :

وهم مجموعة من الأشخاص الذين يقومون بالتسلل إلي نظم المعلومات بغرض الاطلاع عليها وإلحاق الضرر أو العبث بها أو سرقتها . ولقد استفادت هذه الطائفة كثيرا من التقنيات التي طورتها الطائفة السابقة ولكن يتم استخدامها بطريقة سيئة . وتتميز هذه الفئة بالتواصل فيما بينهم والتشاور وعمل المؤتمرات لتطوير طرق الاختراق [3].

٣- المحترفون :

---

[1] - د. ذيب بن عايض القحطاني ، " أمن المعلومات " ، المملكة العربية السعودية ، مدينة الملك عبد العزيز للعلوم والتقنية KACST ، الرياض ٢٠١٥ ، ص ٦٣- ٧٠ .

[2] - ريتشارد مانسفيلد " حيل وأساليب الهاكرز وطرق الوقاية منها " ، ترجمة الدكتور خالد العامري ، القاهرة : الهيئة المصرية العامة للكتاب ، ٢٠٠٦ ، ص٣٤ .

- د. خالد بن سليمان الغثبر ، د.م. محمد عبدالله القحطاني ، " أمن المعلومات بلغة مسيرة " ، مركز التميز لأمن المعلومات ، جامعة الملك سعود ، ٢٠٠٩ ، ص ٢٨ .

[3] - ريتشارد مانسفيلد " حيل وأساليب الهاكرز وطرق الوقاية منها " ، مرجع سبق ذكره ، ٢٠٠٦ ، ص٣٥ .

هذه الفئة تتميز بالتخطيط والتنظيم للجرائم التي ترتكبها ، ولذلك تعد هذه الطائفة أخطر أنواع مجرمي الكمبيوتر والإنترنت ، حيث تهدف هذه الفئة من اختراق أنظمة المعلومات إلي تحقيق الكسب المادي لهم وتحقيق أغراض الجهات التابعين لهم ، والتي قد تهدف إلي تحقيق أغراض سياسية أو التعبير عن موقف فكري معين أو الإرهاب [١]. وتتسم هذه الطائفة بالتكتم علي عكس فئة الكراكرز ، وقد تتراوح أعمار هذه الطائفة ما بين ٢٥ – ٤٠ عام .

٤- الحاقدون :

يكون الدافع لهذه الطائفة هي الرغبة في الانتقام والثأر وليس بهدف تحقيق الذات أو الكسب المادي كما في الطوائف السابقة ، كأن يتصرف بعض العاملين للثأر من تصرف معين لصاحب العمل أو لتصرف المؤسسة المعنية معهم عندما لا يكونون موظفين فيها . ولذلك يتم تقسيمهم إلي فريقين ، الأول مستخدمي للنظام بكونهم موظفين أو مشتركين أو علي علاقة ما بالنظام محل الجريمة (المهاجمون من الداخل) ، الثاني غرباء عن النظام تتوفر لديهم أسباب للانتقام من المؤسسة المستهدفة (المهاجمون من الخارج) [٢] . ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية ، ومع ذلك يسعي الفرد منهم بكل الطرق للوصول إلي معرفة كافة عناصر المعرفة المتعلقة بالعمل الانتقامي الذي ينوي ارتكابه. وتغلب علي هذه الفئة استخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم أو اتلاف كل أو بعض محتوياتها ، أو نشاط إنكار الخدمة من خلال تعطيل النظام او الموقع المستهدف إذا كان من مواقع الانترنت.

تصنيف الهجمات الإلكترونية علي أساس طرق أو كيفية الوصول إلي الأنظمة:

ويطلق علي عملية النفاذ الي المعلومات بطريقة غير مصرح بها بالاختراق . والاختراق بشكل عام هو القدرة علي الوصول لهدف والدخول علي الأجهزة بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص به بهدف التطفل علي خصوصيات الآخرين والحاق الضرر بهم . ويتم اختراق الأنظمة المعلوماتية عن طريق ما يعرف بالهجمات الالكترونية . ويمكن تصنيف الهجمات الالكترونية علي أساس القائم بها أو المصدر ، وايضا يمكن التصنيف علي أساس الغرض منها ، كما يمكن تصنيفها علي أساس طرق أو كيفية الوصول إلي الأنظمة . و فما يلي عرض لهذه التصنيفات .

أ- تصنيف الهجمات الإلكترونية من حيث مصدر الهجمات :

---

[١] - د. خالد بن سليمان الغثبر ، د.م. محمد عبدالله القحطاني ، مرجع سبق ذكره ، ٢٠٠٩ ، ص ٣١ .

[٢] - نفس المرجع السابق ، ص ٢٩ .

١- هجمات خارجية .

ويطلق علي المهاجمين لقب المدمرين (المتلصصين) ومعروف عنهم أن لديهم شغف في تحدي الأنظمة الأمنية للمواقع ، و المتلصصين لديهم القدرة علي الدخول علي المواقع وبالتالي علي الأنظمة والمعلومات والعبث بها من خلال الخادم الذي يقوم بتشغيل النظام أو العبث في المحتويات الفعلية لصفحات الموقع.
كما أن التصنت الإلكتروني هو الآخر محتمل جدا من قبل المتلصصين نتيجة أنه يمكن الحصول علي بعض البيانات والمعلومات الإلكترونية المتسربة من أجهزة الكمبيوتر والبعض الآخر من تسريبات توصيلات الشبكة و تجميعها لتصبح بيانات ومعلومات ذات فائدة ، لذا يجب علي الشركات والمؤسسات أن تحتفظ بأنظمتها الحساسة في أماكن مزودة بنظام أمني لمنع التسرب في المعلومات .

٢- الهجمات الداخلية .

تتم الاختراقات الداخلية (اختراق الأنظمة الأمنية) من قبل شخص داخل الشركة او المؤسسة ذاتها والذي من المحتمل أن يكون من الأشخاص المخول لهم بالدخول إلي عناصر النظام سواء معدات ، أجهزة أو البرامج . والاختراقات الداخلية تعتبر من بين أكثر القضايا التي تواجه المنشآت خطورة وأهمية ولا فرق في مدي الخطورة بين أن يكون مصدر الاختراق من داخل أو خارج المنشأة . وبناء علي ذلك فإنه لا يجب أن يحصل نفس الشخص في نفس الوقت علي صلاحيات للدخول علي الأنظمة التي تشتغل فعليا والأنظمة الاحتياطية معا ، وبصفة خاصة ملفات البيانات والبرامج لأجهزة الكمبيوتر وكذلك أنظمة التشغيل وتطوير وتصميم الأنظمة ، التطبيقات وقواعد البيانات وغيرها .
وعلي ذلك يجب تطبيق الاحترازات الأمنية الفعلية والشفرات الأمنية بشكل أساسي للأشخاص والمسئولين في المنشآت وذلك للتحكم والحد من الأنشطة غير الشرعية ، وبالتالي فإن استخدام التكنولوجيا المتطورة والمختلفة سيقود حتما لتقليل المخاطر من الهجمات الداخلية كما يتيح حماية ضد أنواع كثيرة أخري من الهجمات . والحلول التكنولوجية الشائعة تتضمن كشف الاختراقات ، ومتابعة محاولات الاتصال بالنظام والأحداث الخاصة به ، والتحكم بإصدارات البرامج .

ب- تصنيف الهجمات الإلكترونية من حيث الغرض من الهجمات:

١- هجوم التصنت علي الرسائل Interception Attacks :

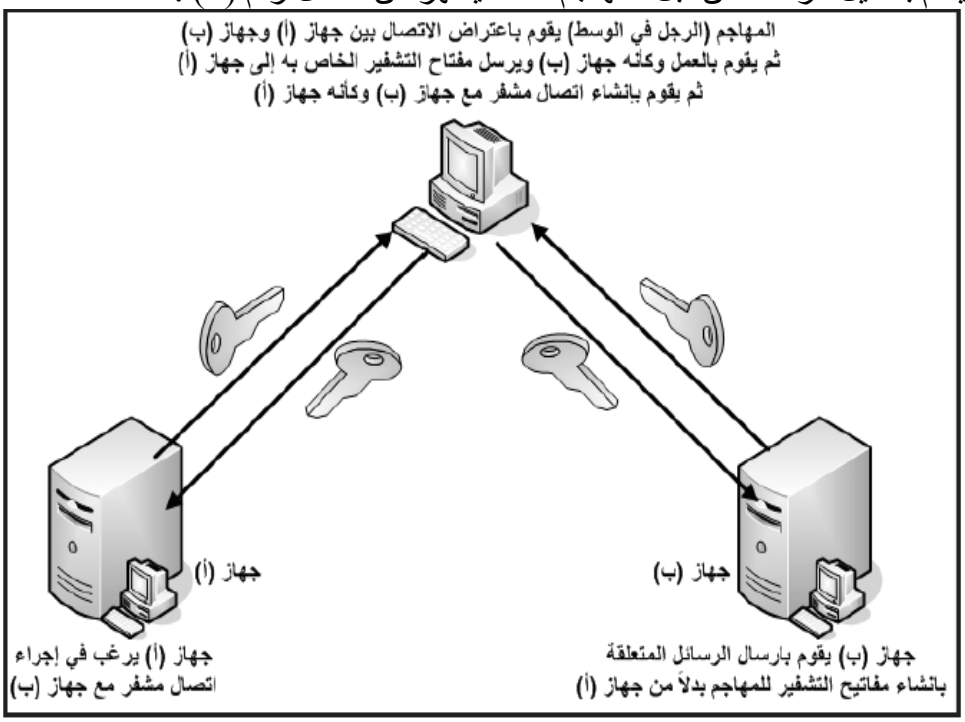
وفكرة عمل هذا الهجوم : ان المهاجم أو المخترق يراقب الاتصال بين المرسل والمستقبل للحصول علي المعلومات السرية وهو ما يسمي بالتصنت علي الاتصال (Eavesdropping) .

٢- هجوم الإيقاف Interruption Attacks :

وهذا النوع من الهجوم يعتمد علي قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلي المستقبل وهو ما يسمي أيضا برفض الخدمة (Denial of service) .

٣- هجوم بغرض تعديل محتوي الرسالة Modification Attacks :

وهذا النوع من الهجوم يتدخل المهاجم بين المرسل والمستقبل بحيث يعتبر المهاجم وسيط بين المرسل والمستقبل ، وعندما تصل الرسالة إلي المهاجم فإنه يقوم بتغيير محتوي الرسالة ومن ثم إرسالها إلي المستقبل ، والمستقبل طبعا لا يعلم بتعديل الرسالة من قبل المهاجم ، كما يظهر من الشكل رقم (٤) .



الشكل رقم (٤) يعرض الهجوم بغرض تعديل محتوي الرسالة

٤- الهجوم المزور أو المفبرك Fabrication Attacks :

وهنا يرسل المهاجم رسالة مفادها أنه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة مثلا .

جـ- تصنيف الهجمات الإلكترونية من حيث طرق أو كيفية الوصول إلي الأنظمة الهجمات:

١- هجمات البرامج واستخدام الأكواد الخبيثة .

وتتمثل في هجمات الفيروسات ، وبرامج أحصنة طروادة ، وبرامج الاختراق ،وبرامج التجسس الإلكتروني ، وقد تتسبب هذه البرامج في أضرار كثيرة تتراوح ما بين مجرد الإزعاج ، إلي فقد البيانات ،و وصولا إلي سرقة الأموال . وللحد من هذه المخاطر يجب توفير أنظمة الكترونية حديثة لمكافحة هذه البرامج والعمل علي تحديثها بصفة مستمرة وتدريب العاملين عليها .

٢- هجمات الأبواب الخلفية .

قد يترك المصممون أو المبرمجون أو فنيو الصيانة طرق خفية ، تسمي الأبواب الخلفية ، وذلك للوصول إلي الأجهزة والشبكات من أجل استخدامها لاحقا لأعمال التطوير والصيانة عن بعد ، ويستغل الهاكرز هذه الطرق عند اكتشافها للدخول إلي الأجهزة والشبكات بطرق غير شرعية . وهذه الأبواب الخلفية يكون من الصعوبة بمكان اكتشافها لأنها عادة لا تكون تحت نظر برامج وأنظمة المتابعة والمراجعة ، وإنما هي أبواب خفية حتي علي هذه الأنظمة . ولذلك تبرز الحاجة إلي آليات وطرق الحماية اللازمة لكشف هذه الأبواب وترشيد وتقنين استخدامها أو منعها بالكلية .

٣- هجمات المتشمم أو الالتقاط Sniffer Attacks [١]:

المتشمم هو برنامج أو جهاز يراقب البيانات المارة عبر الشبكة ويلتقطها . ويعد هذا الهجوم خطيرا جدا علي الشبكة لأنه يمكن زرع المتشمم في أي مكان في الشبكة ، وغالبا لا يمكن كشفه ، وهذا ما يجعله محببا لدي المهاجمين . ويستطيع المتشمم قراءة كلمات المرور وكذلك محتويات الملفات النصية وخاصة اذا كانت الشبكات غير مشفرة . لذلك يجب توفير أنظمة حماية تكشف وجود برامج وأجهزة التشمم وتكافحها ، العمل علي تشفير الملفات والأنظمة للحد من الاستفادة من المعلومات المسروقة في حالة نجاح المتشمم في سرقتها .

٤- هجمات الهندسة الاجتماعية [٢]:

يعتمد هذا النوع من الهجوم علي كسب ثقة الضحايا وإيهامهم بأن من يطلب منهم معلوماتهم السرية (كاسم المستخدم وكلمة المرور وأرقام بطاقات الائتمان) هو جهة موثوقة (بنك مثلا) وبعد ذلك يتم استغلال هذه المعلومات وانتحال شخصيات الضحايا ومن ثم سرقتهم إلكترونيا عن طريق دخول يبدو شرعيا لأنظمة الحماية . ومن الأمثلة الشهيرة علي هذا النوع من الهجوم هو هجمات الاصطياد الإلكتروني .

٥- هجوم تصفح الكتف :

---

[١] - خالد بن سليمان الغثبر ، محمد بن عبد الله القحطاني ، مرجع سبق ذكره ، ٢٠٠٩ ، ص ٣٣ .

[٢] - خالد بن سليمان الغثبر ، سليمان بن عبد العزيز بن هيشة ، " الاصطياد الإلكتروني : الأساليب والإجراءات المضادة " ، مركز التميز لأمن المعلومات ، جامعة الملك سعود ، ٢٠٠٩ ، ص ٤١ .

ويعني هذا الهجوم أن يضطلع المهاجم علي المعلومات المهمة والحساسة كما لو كان ينظر إليها من فوق كتف الضحية ، ويري لوحة المفاتيح وما يقوم بضغطه من أزرار وما يعرض علي الشاشة من معلومات . وعادة ما يستخدم هذا الهجوم في الأماكن العامة أو اماكن العمل المشتركة ، حيث ينظر المهاجم خلسة إلي شاشة الضحية ، ومن ثم يعرف بعض المعلومات السرية التي يجب أن لا يعرفها مثل النظر خلسة إلي الأرقام السرية لبطاقات الصراف الآلي وقت إدخال مستخدمها لها ، معرفة كلمات المرور للحاسبات الآلية ، وأرقام الهواتف وقت إدخالها .

٦- هجمات المعلومات الجانبية [١]:

يعتبر من أخطر أنوع الهجوم حيث يعتمد المهاجم علي المعلومات التي يجمعها المهاجم من أجهزة التشفير وخاصة أجهزة التشفير التي تعمل بأنظمة التشفير بالمفتاح العام ، ثم يقوم بتحليلها للحصول علي المعلومات السرية كمفاتيح التشفير . وما يحدث ليس كسرا لأنظمة التشفير بشكل مباشر بل جمع المعلومات الجانبية مثل الوقت المستغرق أو كمية الطاقة الكهربية المستهلكة لإتمام عملية حسابية معينة .

المحور الرابع : عناصر و وسائل أمن المعلومات

أولا : عناصر أمن المعلومات :

يمكن تعريف عناصر أمن المعلومات بأنها " مجموعة العناصر الواجب توافرها لحماية المعلومات الثابتة والمنقولة ، بحيث يغطي كل عنصر من هذه العناصر جانبا من جوانب الحماية المطلوبة " [٢]. وهذا التعريف يوضح التكامل الواضح بين عناصر أمن المعلومات ، حيث أن فقدان أحد هذه العناصر يؤدي إلي خلل أمني يمكن من خلاله الوصول غير المصرح به إلي هذه المعلومات . و يهدف أمن المعلومات إلي المحافظة علي سلامة وخصوصية المعلومات المتداولة عبر الانترنت من الفقد او التلف أو الوصول غير المسموح به لهذه المعلومات .

لا يوجد اتفاق عام علي الركائز الأساسية التي يقوم عليها أمن المعلومات حيث يري البعض أن أمن المعلومات يقوم علي ثلاث ركائز أساسية لأمن المعلومات وهي : السرية (confidentiality) ، التكاملية وسلامة المحتوي (Integrity) ، توافر المعلومات (Availability) وقد أطلق علي هذه

---

[1] - Mangard et. al.(2007), "Power Analysis Attacks: Revealing the Secrets of Smart Cards", Springer Science and Business Media, LCC, 2007,p8.

[٢] - د. ذيب بن عايض القحطاني ، " أمن المعلومات " ، مرجع سبق ذكره ، ٢٠١٥ ، ص ٧٨ .

العناصر الثلاث مثلث (CIA)[1]. إلا أن الاتحاد العالمي للاتصالات في توصيته X.800 قد حدد سبعة عناصر أساسية لأمن المعلومات وهي : التحقق من الهوية ، والتحكم بالوصول ، السرية ، سلامة المعلومات وتكاملها ، عدم الإنكار ، توافر أو ديمومة المعلومة ، المتابعة أو المراجعة [2]. وسوف نتناول كل عنصر من عناصر أمن المعلومات كما يلي :

١- **التحقق من الهوية Authentication** : تعني الخدمة التي يمكن من خلالها التحقق من هوية الشخص (أو الجهة) وأنه الشخص المعني لا غيره. ويطلق أيضا علي التحقق من الهوية " المصادقة " وتعني أن جميع الاتصالات موثوقة [3]. وتحدد توصية X.800 شقين رئيسيين للتحقق من الهوية وهما :

- التحقق من هوية الشخص أو الجهة : ويوفر التحقق من هوية طرفي الاتصال في جميع مراحله وضمان عدم قدرة المتعدي علي انتحال شخصية أحد طرفي الاتصال . ويجب التحقق من هوية طرفي الاتصال في كل عملية منفردة .
- التحقق من أصل منشأ المعلومة : تأكيد مصدر المعلومة .

ويمكن استخدام معيار أو أكثر للتحقق من الهوية حسب درجة التحقق المطلوبة ، كما يلي :

- التحقق باستخدام معيار واحد : هذا المعيار " ماذا تعرف؟" . ويعتمد هذا المعيار علي طلب (ادخال) معلومة لا يعرفها إلا الشخص المعني فقط ، كاستخدام كلمات المرور أو أرقام التعريف الشخصية . ويعد ذلك من أدني درجات التحقق من الهوية .
- التحقق باستخدام معيارين : ويتم ذلك باستخدام معيار " ماذا تعرف؟" بالإضافة إلي معيار آخر هو " ماذا تملك ؟ "، مثل استخدام بطاقات الصراف الآلي حيث يتم التحقق من هوية الشخص من خلال رقم البطاقة التي لا يملكها إلا هو ، ثم إدخال الرقم السري الذي لا يعرفه إلا هو كذلك ، ولا يمكن أن يغني أحدهما عن الأخر . ويوفر التحقق

---

[1] - اتحاد المصارف العربية ، " أمن المعلومات : المخاطر وتحديات المستقبل " ، الأمانة العامة – إدارة الدراسات والبحوث ، ٩/٤/ ٢٠١٨ ، ص ١.

2 - Stallings, William (2007), "Network Security Essentials: Applications and Standards", Third Edition, Prentice-Hall, 2007, p 23.

3 - Stallings, William (2006), "Cryptography and Network Security: Principles and Practices", Fourth Edition, Prentice-Hall, 2006, p33.

باستخدام معيارين درجة جيدة من درجات التحقق من الهوية أعلي من التحقق باستخدام معيار واحد .

- التحقق باستخدام ثلاثة معايير : ويتم ذلك باستخدام معيار " ماذا تعرف؟" و معيار " ماذا تملك ؟ "وإضافة معيار ثالث هو " من أنت؟" .

وتعتمد هذه الطريقة في التحقق من الهوية علي طلب معلومة لا يعرفها إلا الشخص المعني فقط ، ومعلومة أخري لا يملكها إلا الشخص نفسه ، ومعلومة ثالثة من واحدة أو أكثر من خصائص الشخص الحيوية التي تميزه عن غيره مثل بصمة العين أو الأصابع والصوت وابعاد راحة اليد وغير ذلك . وهذه الطريقة توفر أعلي درجات التحقق من الهوية ولكنها تحتاج إلي أجهزة وبرامج إضافية حيث انها تعد أكثر تعقيدا من سابقاتها.

٢- **التحكم بالوصول Access Control :** هي طرق الحماية التي تمنع الاستخدام غير المرخص به لموارد المنشأة كالأجهزة الرئيسية والبيانات المركزية . وهذه الطرق تحمي من الوصول غير الشرعي وتساعد علي تحديد مستوي التخويل المصرح به (Authorization) بعد نجاح عملية التحقق من الهوية .

يعد التحكم بالوصول من أوائل خطوط الدفاع عن موارد المنشأة. فيمكن اعتبار ان مجرد ادخال "اسم المستخدم" و "كلمة المرور" هو تحكم بالوصول الى ملف معين، وهذا الملف لديه قائمة بالمستخدمين و المجموعات المسموح لهم بالوصول اليها فاذا لم يكن ذلك المستخدم من ضمن تلك القائمة، فلن يسمح له. كذلك الحال لموارد المنشأة الأخرى، كالأجهزة والطابعات ، وقواعد البيانات ، والماسحات الضوئية وغير ذلك من الموارد المتاحة. ومن ثم يمكن القول ان التحكم بالوصول يعطى المنشأة امكانية تقييد استخدام مواردها ومراقبة ذلك الاستخدام.

ولكى يتمكن المستفيد(مستخدم او برنامج او عملية او غيره) من الوصول الى مورد ما، واستخدامه، او الاستفادة منه، فانه يجب ان يمر بمرحلتين قبليتين للتحكم بوصوله الى ذلك المورد هما: التحقق من الهوية، والتخويل، ثم مرحلة ثالثة بعد وصوله للمورد واستخدامه وهي المتابعة والمراجعة .

٣- **السرية (confidentiality)** - وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها أحد من غير المرخص لهم بذلك . وقد يستطيع الهاكرز إحباط فاعلية عنصر السرية باستخدام عدة طرق من أهمها : مراقبة الشبكة ، وهجوم تصفح الكتف ، والهندسة الاجتماعية. وقد يكشف المستخدم عن بعض المعلومات الحساسة عمدا ، أو عن طريق الخطأ عندما لا يقوم بتشفير

هذه المعلومات ، أو عندما يقع ضحية لهجمات الهندسة الاجتماعية ، او بسبب اللامبالاة والاهمال وغياب الحس الأمني عند معالجة هذه المعلومات .

٤- **التكاملية وسلامة المحتوي (Integrity)** - وتعني التأكد من أن محتوي المعلومات صحيح ولم يتم التعديل أو العبث بأية مرحلة من مراحل التخزين أو المعالجة. ولا يهتم عنصر سلامة المعلومات وتكاملها بضمان دقة المعلومات وسلامتها فحسب ، بل يعني كذلك بدقة الأنظمة المعالجة لها وسلامتها من التلاعب أو التغيير غير المصرح به ، ويتطلب ذلك أن تعمل الأجهزة والبرامج وأنظمة الشبكات بانسجام تام للمحافظة علي المعلومات ومعالجتها ونقلها إلي وجهتها الصحيحة دون أي تغيير ، او تعديل . ويشمل كذلك الحفاظ علي البيانات من أي تلويث خارجي ، أو تداخل ، أو تضارب ، او تشويش مع بيانات أخري . و يراعي في هذا المجال ما يلي [١]:-

- إتباع سياسات و إجراءات تحقق تأمين الاتصالات من و إلي النظم لمنع أو الحد من اختراق غير المرخص لهم للنظم أو إساءة استخدامها.
- الرقابة علي دخول النظم و تحديد شخصية المستخدمين.
- حماية النظم من احتمالات القيام بممارسات غير مرخص بها من قبل العاملين بالمنشأة السابقين أو الجدد أو المؤقتين.

٥- **عدم الإنكار Non- Repudiation** : هي الخدمة التي من خلالها يمكن منع أي شخص أو جهة من إنكار أي عملية قاموا بها وكشفهم ، من خلال ايجاد أدلة قاطعة علي تصدير أو تسليم البيانات لحماية المرسل من عدم الاعتراض الغير صحيح من قبل المستلم (المستقبل) بعدم استلام البيانات ، وبأنها أستملت أيضا لحماية المستلم من عدم الاعتراض الغير صحيح من قبل المرسل بأن البيانات فعلا قد تم ارسالها .ويلعب عنصر عدم الانكار دورا رئيسا في إثبات وقوع العمليات التفاعلية (بين طرفين) كالعمليات المالية ، وعمليات الحكومة الإلكترونية . وتشمل خدمة عدم الانكار إثبات وقوع العمليات الإلكترونية في أوقات وتواريخ معينة عن طريق الحاق بصمة التاريخ والوقت بالعملية نفسها (Time Stamping) .

٦- **توافر المعلومات (Availability)** – التأكد من استمرار عمل نظم المعلومات واستمرار القدرة علي التفاعل معهم من قبل المستخدمين ، وان تكون المعلومات متاحة لكافة الأشخاص المخول لهم بالتعامل مع البيانات والمعلومات .

---

[١] - البنك المركزي المصري ، " الضوابط الرقابية للعمليات المصرفية الالكترونية وإصدار وسائل دفع لنقود الكترونية " ، البنك المركزي المصري ، ٢٨ فبراير ٢٠٠٢ ، ص ٦ .

إن الهدف العام من عنصر توافر المعلومات هو أن تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج إليها المستخدم ، وأن توفر لها الحماية مما قد يتسبب في عطل أو عدم توافر أي منها ، وفي حالة حدوث الأعطال أو الكوارث المعلوماتية يجب أن تكون هناك شبكة وأجهزة وأنظمة وبرامج بديلة يجري إحلالها آليا و بسرعة فائقة محل تلك التي تعرضت للعطل أو الكارثة ، وفق خطة تشغيل للطوارئ يتم إقرارها والتدريب عليها جيدا قبل ذلك . وتجدر الإشارة إلي أنه لابد من الموازنة بين الحماية وتوافر المعلومات [١]. و لذلك يتعين علي المنشآت ما يلي :-

- أن تحدد الآليات البديلة لاستئناف الخدمة في حال أي توقف. و يجب توجيه اهتمام خاص للقدرة علي استرجاع السجلات الإلكترونية و المادية الضرورية لاستئناف الأعمال.
- أن تقوم بمراجعات دورية لخطط الطوارئ و مواصلة الأعمال حتى تكون متسقة مع العمليات الجارية للمنشأة و خططها الاستراتيجية. و يجب علاوة علي ذلك إخضاع الخطط لاختبارات دورية لضمان قدرة المنشأة علي تنفيذها في حال التعرض لتوقف خطير في الأعمال[٢] .
- كما يتعين علي المنشآت إيجاد بدائل في حالة الاعتماد علي المورد الخارجي في توفير هذه الخدمات.
- كما يجب الأخذ في الاعتبار حدوث أعطال ما في شبكة الإنترنت و العمل علي تبني خطط للطوارئ في هذه الحالة.
- قد يكون من المفيد التعاقد مع أحد بيوت الخبرة لاكتشاف الخلل في الأنظمة و بصورة دورية و ذلك للحد من الهجمات التي قد تساهم في تعطيل انتظام الخدمة.

٧- المتابعة أو المراجعة Auditing :

تهدف المتابعة إلي متابعة عمليات المستخدمين والتحقق من فرض سياسات أمن المعلومات ، وأنها تطبق بشكل دقيق . كما يمكن استخدام نتائج المتابعة كأدوات تحقيق في حال خرق لأنظمة أمن المعلومات لإثبات وقوع هذا الخرق ، وإثبات إدانة المستخدم (أو المتهم) أو براءته من القيام بذلك الحدث .

---

[١] - د. ذيب بن عايض القحطاني ، " أمن المعلومات " ، مرجع سبق ذكره ، ٢٠١٥ ، ص ٩٦ .

[٢] - اللجنة العربية للرقابة المصرفية " إدارة المخاطر التشغيلية و كيفية احتساب المتطلبات الرأسمالية لها " ، ، صندوق النقد العربي ، أبو ظبي ، سنة ٢٠٠٤ ، ص ٢٠ .

ويوجد أسباب ضرورية لإجراء عمليات المتابعة والمراجعة علي موارد الشبكة ومستخدميها منها [1]:

- التحقق من ان الاجهزة و الانظمة و البرامج تعمل بشكل طبيعي من خلال مراجعة سجلات الاحداث (Log Files) ، ثم اتخاذ الإجراءات المناسبة ، بناء على المعلومات المتوافرة في تلك السجلات .
- مراقبة العمليات الضارة التي قد يقوم بها المستخدمون عمدا كان أو بالخطأ.
- الكشف عن عمليات التطفل و الاختراقات.
- المساعدة على استعادة الاحداث ومعرفة متطلبات الأنظمة واعداداتها، لاستعادتها كما كانت قبل وقوع أي مشكلة.
- تشكل مصدرا قانونيا رسميا للمنشأة لإثبات الأحداث أو نفيها.
- تشكل مصدرا من مصادر التقارير الرسمية للمنشأة عن انشطتها والمشكلات التي قد تقع فيها، أو في انظمتها.

ثانيا: وسائل أمن المعلومات .

هناك تقنيات رئيسية يمكن استخدامها كوحدات بناء أساسية لتحقيق عناصر أمن المعلومات وهي :

- التشفير Encryption .
- التصريح الرقمي Digital Authorization
- تسجيل الدخول الواحد Single Sign-on
- مصفوفة التحكم بالوصول Access Control Matrix
- أنظمة كشف التطفل Intrusion Detection Systems
- أنظمة منع التطفل Intrusion Prevention Systems

وتستخدم هذه الوسائل لتحقيق عناصر أمن المعلومات . حيث يتم تحقيق عنصر السرية باستخدام تقنية التشفير بنوعيه ، ويمكن التحقق من الهوية ، التحكم بالوصول (للمنشآت الصغيرة) ، وعدم الإنكار باستخدام التشفير غير المتماثل (المتناظر) والتصديق الرقمي معا . ويمكن تحقيق عنصر سلامة المعلومات وتكاملها باستخدام البصمة الرقمية . كما يمكن استخدام التصديق الرقمي من التحقق من هوية الشخص ، ويستخدم مع البصمة الرقمية للتحقق من هوية الرسالة أو المعلومة . كما يمكن استخدام تقنيات تسجيل الدخول ،ومصفوفات قوائم التحكم ، وأنظمة كشف ومنع التطفل لتحقيق عنصر التحكم بالوصول

[1] - د. ذيب بن عايض القحطاني ، " أمن المعلومات " ، مرجع سبق ذكره ، ٢٠١٥ ، ص ٩٧ - ٩٨.

للمنشآت الكبيرة والمنشآت التي تحتاج إلي أنظمة تحكم بالوصول قوية متخصصة في ذلك .
ويتم استخدام الأجهزة والبرامج وأنظمة الحماية ضد الهجمات والتي تعطل الخدمة Denial of Service ، وتحقيق عنصر المراجعة باستخدام تقنيات متابعة وتسجيل الأحداث ، سواء تلك التي ترد رفق أنظمة التشغيل أو التي يتم بنائها من قبل شركات متخصصة في ذلك . وسوف نتناول كل من هذه الوسائل أو التقنيات كما يلي :

١- **التشفير Encryption** [١]**:** يعتمد التشفير علي تغيير محتوي الرسالة باستخدام أسلوب محدد (برنامج محدد) يسمي مفتاح التشفير وذلك قبل إرسال الرسالة علي أن تكون لدي المستقبل القدرة علي استعادة محتوي الرسالة في صورتها الأصلية قبل التشفير باستخدام العملية العكسية لعملية التشفير Encryption والتي تسمي الحل Decryption .

نظم التشفير : وهي النظم التي يمكن بها تشفير الرسائل وفك تشفير هذه الرسائل بين المرسل والمستقبل ، وفيما يلي نستعرض كل نوع من هذه الأنواع بشيء من الإيجاز كما يلي .

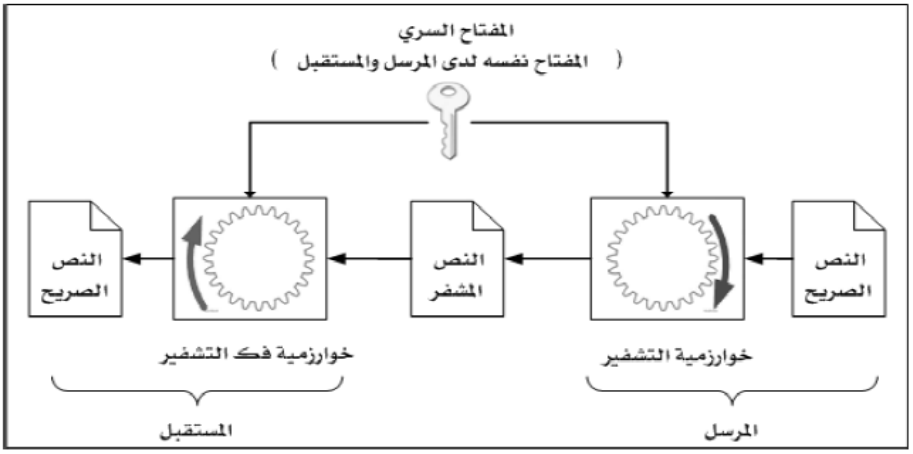
أ - التشفير المتناظر (نظام المفتاح المتماثل) Cryptography[٢]: وتتم عملية التشفير وفك التشفير بنفس مفتاح التشفير حيث تتم العملية كما يلي :

عملية التشفير : يتم عملية تشفير الرسالة (المعاملة) لدي المرسل باستخدام مفتاح خاص Symmetric Key لينتج منها رسالة مشفرة . ويقوم المرسل بإرسال الرسالة المشفرة إلي المستقبل باستخدام وسائل الاتصال العادية ويقوم بإرسال المفتاح باستخدام وسيلة مؤمنة .

عملية فك التشفير : يقوم المستقبل بعد تلقي الرسالة المشفرة والحصول علي المفتاح بحل الشفرة والحصول علي الرسالة الأصلية كما هو موضح بالشكل رقم (٥) .

---

[١] - د/ رأفت رضوان ، " التجارة الإلكترونية " ، القاهرة : المنظمة العربية للتنمية الإدارية ، ١٩٩٩ ، ص ٨٠ .
[٢] - د/ رأفت رضوان ، " التجارة الإلكترونية " مرجع سبق ذكره ، ١٩٩٩ ، ص ٨٤ -٨٥ .



شكل رقم (٥)
يوضح نظام تشفير المفتاح المتماثل

ب- نظام التشفير بالمفتاح العام Public Key Encryption[١].

كانت المشكلة الأساسية في نظام التشفير المتناظر هي كيفية الحصول علي المفتاح نفسه لكل من المرسل والمستقبل ، أو ما يسمي بمشكلة توزيع المفاتيح . ولحل هذه المشكلة جرى تطوير التشفير باستخدام المفتاح العام .

قدم التشفير باستخدام المفتاح العام طريقه جديدة تختلف تماما عن التشفير المتناظر، حيث لا يوجد مفتاح سرى مشترك بين المرسل والمستقبل منذ البداية، وانما يستخدم مفتاحان منفصلان، يستخدم احدهما للتشفير، والآخر(وهو مرتبط بالأول) لفك التشفير.

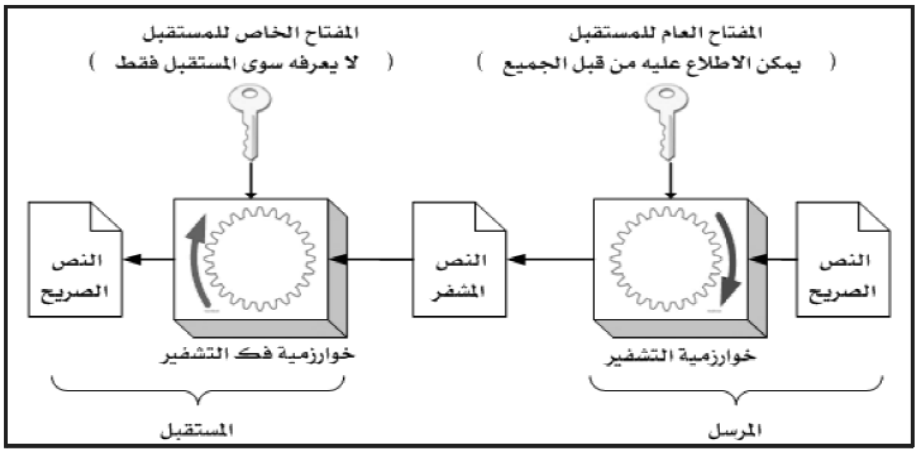
في هذا النوع من التشفير، يولد كل مستخدم زوجا من المفاتيح مرتبطين بعضهما ببعض (بطريقه رياضيه معقده لا تسمح بكشف أي منهما اذا عرف الاخر) احدهما عام ويوضع في سجل (مجلد) عام يمكن الاطلاع عليه من قبل جميع المستخدمين، والاخر خاص ويعد مفتاحا سريا خاصا بالمستخدم ويجب الا يطلع عليه الآخرون. ثم بعد ذلك تتم عمليتا التشفير وفق الاتي:

- **عملية التشفير:** تشفر الرسالة الاصلية باستخدام خوارزمية التشفير والمفتاح العام للمستقبل للحصول على رسالة مشفرة.
- **عملية فك التشفير:** يتم فك تشفير الرسالة المشفرة باستخدام خوارزمية فك التشفير والمفتاح الخاص (السرى) للمستقبل؛ للحصول على الرسالة

---

[١] - أ- د. ذيب بن عايض القحطاني ، " أمن المعلومات " ، مرجع سبق ذكره ، ٢٠١٥ ، ص ١٤٥- ١٤٨ .
ب- د/ رأفت رضوان ، " التجارة الإلكترونية " مرجع سبق ذكره ، ١٩٩٩ ، ص ٨٥ -٨٧ .

الاصلية، وبهذه الطريقة لن يستطيع أي شخص اخر فك تشفير الرسالة؛ لأنه لا يملك المفتاح الخاص للمستقبل. كما هو موضح بالشكل رقم (٦).



شكل رقم (٦) يوضح نظام تشفير المفتاح العام

و يجب ان يملك جميع المشتركين في نظام التشفير غير المتناظر حق الوصول الى المفاتيح العامة واستخدامها في التشفير، ويتم توليد المفاتيح الخاصة محليا لدى كل مستخدم (بشكل آلي) و من ثم فليس هناك حاجه لتوزيع المفاتيح كما هي الحال في التشفير المتناظر، ويمكن لأي مستخدم تغيير مفتاحه الخاص في أي وقت شريطة انتاج المفتاح العام الموافق له، ووضعه في السجل المشترك (العام) ، بحيث يطلع عليه جميع المستخدمين.

٢- التصريح الرقمي Digital Authorization

ويتعلق بالتقنيات التي تدعم عملية أمن المعلومات حيث تمثل تقنيات تعمل علي تحقيق بعض عناصر أمن المعلومات وبالأخص التحقق من الهوية ، والسرية ، وعدم الإنكار **وتشمل تقنيتين هما :**

١/٢- التوقيع الرقمي Digital Signature :

يعتبر التوقيع الرقمي أحد أهم أدوات أمن المعلومات ، حيث يعد وحدة بناء أساسية لتحقيق عدد من عناصر أمن المعلومات ، مثل التحقق من هوية أصل البيانات (المرسل) ، وعدم الإنكار .

ويعتمد التوقيع الرقمي بشكل أساسي علي نظام التشفير بالمفتاح العام ولكن بطريقة عكسية له . حيث يتم توقيع الرسالة من قبل المرسل باستخدام مفتاحه السري الخاص به (وليس المفتاح العام للمستقبل كما هو الحال في التشفير بالمفتاح العام) ، ويتم التحقق من صحة التوقيع من قبل مستلم الرسالة

(المستقبل) باستخدام المفتاح العام للموقع [1]. وبذلك يسمح التوقيع الالكتروني للشركات بتبادل المعلومات الحساسة والهامة بدون الخوف من دخول أطراف خارجية في عملية التبادل ولا شك أن هذه التقنية تستخدم في البنوك والمؤسسات المالية المختلفة والقطاعات العامة والحكومات وغيرها.

٢/٢- الشهادات الرقمية [٢] Digital Certificate .

تصدر هذه الشهادة من جهة تسمي جهة الاعتماد Certificate Authority وتقر بأن صاحب الرسالة أو المعاملة هو الشخص ذاته المحدد بهذه الرسالة .

الشهادات الرقمية هي ملفات تستخدم لأغراض الأمن الالكتروني تتضمن اسم وعنوان صاحب الشهادة وتاريخ التصريح ومفتاح التشفير العام المستخدم في الوثيقة والذي من خلاله يتم التعرف على التوقيع الالكتروني والتأكد من صلاحيته ،وتاريخ انتهاء صلاحية هذه الشهادة . بالإضافة إلى اسم الشركة التجارية ويستخدم في العادة نظام Secure Sockets Layer (SSL) والذي يضمن الاتصال الآمن بين مستخدم الشبكة ومقدم الخدمة وهي تقنية أمنية تستخدم في العادة لتشفير الاتصالات بين المستخدمين ومواقع التجارة الالكترونية والذي يؤمن التبادلات التجارية بينهما ويمنع أي تدخل خارجي على هذه البيانات.

٣- تسجيل الدخول الواحد Single Sign-on

تستخدم تقنية تسجيل الدخول الواحد Single Sign-on بدلا من استخدام المستخدم الواحد عدة أسماء للمستخدمين وكلمات مرور مختلفة للدخول إلي نظام التشغيل ،والشبكات والبرامج التطبيقية . حيث يدخل المستخدم مرة واحدة من خلال نظام موحد مخصص لهذا الغرض (مثل نظام كيربورس Kerberos) ، وبذلك تكون جميع موارد الشبكة التي يحتاجها في متناوله ، وفق الصلاحيات الممنوحة له . وقد يبدو للوهلة الأولي أن هذه الطريقة تؤدي إلي ضعف أمن المعلومات ، لكن الواقع يشير إلي انها تعمل علي تقوية أمن هذه الأنظمة ، لأن المستخدم الذي لديه عدد كبير من أسماء المستخدمين وكلمات المرور عادة ما يضطر إلي تسجيلها في مذكرة أو في حسابه الشخصي ، لتسهيل عملية الرجوع إليها وتذكرها ، وهذا الأمر ينافي السياسات الأمنية لكلمات المرور وتكون عرضة لاكتشافها من الآخرين .

٤- مصفوفة التحكم بالوصول Access Control Matrix

---

[1] - Bhaskar, S. M., and Ahson S. I., "Information Security: A practical Approach", Alpha Science International LTD, Oxford, U.K., 2008 ,p98- 101.

[٢] - د/ رأفت رضوان ، " التجارة الإلكترونية " مرجع سبق ذكره ، ١٩٩٩ ، ص ١٠١.

وهي عبارة عن جدول يحتوي علي أسماء المستفيدين والموارد التي يستطيع المستفيد التعامل معها ، ويحدد العمليات الممكنة لكل مستفيد علي كل مورد . حيث أن الصف الواحد يحدد اسم مستفيد واحد والعمليات الممكنة لهذا المستفيد علي كل مورد .

٥- أنظمة كشف التطفل Intrusion Detection Systems

يقصد بكشف التطفل عملية كشف الاستخدام غير الشرعي أو الهجوم علي الأجهزة والشبكات وأنظمة الاتصالات ، والمهمة الأساسية لأنظمة كشف التطفل هي التقاط أي شيء مريب أو مشكوك فيه يحدث في الأجهزة والشبكة ، والتنبيه علي ذلك في شكل رسالة إلي مدير النظام . وعادة ما تقوم أدوات كشف التطفل بتفحص سيل البيانات وسجلات الأحداث Log Files ، وكشف أي بيانات غير طبيعية والتنبيه عليها . ويوجد نوعان رئيسيان من أنظمة كشف التطفل هما : أنظمة كشف التطفل علي الشبكة ، وأنظمة كشف التطفل علي الأجهزة . وتتكون أغلب أنظمة كشف التطفل من ثلاثة مكونات رئيسية هي :

- الحساسات Sensors : تجمع البيانات وأنشطة المستخدمين وترسلها لأدوات التحليل .
- أدوات التحليل Analyzing tools : تحلل البيانات والأحداث الواردة اليها من الحساسات وتتعرف علي البيانات والأنشطة التي تبدو غير طبيعية .
- واجهات التواصل مع مديري الأنظمة Interfaces : في حالة وجود أي نتائج لبيانات أو أنشطة مريبة وغير طبيعية ترسل إلي واجهات التواصل مع مديري الأنظمة لإخطارهم بوجود شيء غير طبيعي لاتخاذ الإجراء المناسب .

٦- أنظمة منع التطفل Intrusion Prevention Systems

أنظمة كشف التطفل تكشف عن البيانات والأنشطة غير الطبيعية ، ومن ثم التنبيه عنها فقط ، أما أنظمة منع التطفل فتكشف البيانات والأنشطة غير الطبيعية قبل وصولها إلي أهدافها. وبذلك فإن أنظمة منع التطفل تقوم بخطوات استباقية لمنع المتطفل من الوصول إلي أهدافه .

المحور الخامس
الدراسة الميدانية

أولا : مجتمع وعينة الدراسة .

مجتمع الدراسة : يتمثل مجتمع الدراسة في مسئولي إدارة تكنولوجيا المعلومات بالبنوك التجارية العاملة بمصر ، حيث شهدت السنوات الأخيرة تقدما ملموسا في مجال العمليات المصرفية الإلكترونية نتيجة لتزايد استخدام تكنولوجيا المعلومات داخل البنوك التجارية. و يقصد بالعمليات المصرفية الإلكترونية قيام البنوك

بتقديم الخدمات المصرفية التقليدية أو المبتكرة من خلال استخدام وسائط الاتصال الإلكترونية المفتوحة (الانترنت)[1]. بالإضافة إلي أن الخدمات المصرفية المتاحة عن طريق الإنترنت باستطاعتها أن توفر من تكاليف التشغيل الخاصة بالبنوك والمؤسسات المالية .

عينة الدارسة :

تم تحديد ثلاثة من البنوك التجارية العاملة بجمهورية مصر العربية وهي بنك مصر ، بنك القاهرة ، والبنك الأهلي المصري ، حيث تعد من أكبر وأقدم البنوك التجارية العاملة بمصر وأكثرها استخداما لتكنولوجيا الاتصالات والمعلومات .
وقد قام الباحث بتوزيع ١٤٠ استمارة استقصاء علي الإدارات المركزية في البنوك التي تمثل عينة الدراسة علي الفئات المختصة بالدارسة وهم (مسئولي إدارة تكنولوجيا المعلومات) كما هو موضح بالجدول رقم (٢).

جدول (٢) يوضح عينة الدراسة

	عينة المجال الميداني				النسبة %
	بنك مصر	بنك القاهرة	البنك الأهلي	الإجمالي	
الموزعة	٤٥	٤٥	٥٠	١٤٠	١٠٠
الواردة	٤٠	٣٨	٤٢	١٢٠	٨٥,٧
المستبعدة	٣	٤	٢	٩	٦,٤
الصحيحة	٣٧	٣٤	٤٠	١١١	٧٩,٣

وقد بلغت الاستمارات الواردة من البنوك الثلاثة (١٢٠) استمارة أي بنسبة ٨٥,٧ % من إجمالي عدد الاستمارات الموزعة علي البنوك ، وباقي الاستمارات وعددها ٢٠ استمارة لم يتم تسليمها للباحث من قبل المستقصي منهم كما هو موضح بالجدول السابق . وكان عدد الاستمارات الصحيحة والصالحة لعمل التحليل الإحصائي منهم (١١١) استمارة أي بنسبة استجابة ٧٩,٣ % من إجمالي عدد الاستمارات الموزعة علي البنوك وبلغ عدد الاستمارات غير المستكملة من الاستمارات المستلمة ٩ استمارة بنسبة ٦,٤ % من إجمالي عدد الاستمارات الموزعة علي البنوك كما هو موضح في الجدول رقم (٢).

ثانيا : الأساليب الإحصائية المستخدمة .

١- اختبار قائمة الاستقصاء :-

[1] - البنك المركزي المصري ، " الضوابط الرقابية للعمليات المصرفية الالكترونية " ، البنك المركزي المصري ، ٢٠١٢ ، ص ١ .

تم إجراء اختباري الصدق والثبات لاستمارة الاستقصاء ، بغرض التعرف علي مدي قدرة هذه الاستمارات علي الاستدلال والصلاحية لقياس المفترض قياسه . ويهدف اختبار الصدق إلي الكشف عن الظواهر أو السمات أو الخصائص التي تجري الدراسة من أجلها ، وللتأكد من أن الاستقصاء يوفر المعلومات المطلوبة . بينما يهدف اختبار الثبات إلي قياس اتساق الإجابات علي أسئلة الاستقصاء. وللتحقق من الثبات و الصدق الذاتي لقائمة الاستقصاء المستخدمة في تجميع بيانات هذه الدراسة ، تم تحديد معامل الثبات لقائمة الاستقصاء بحساب معامل كرونباج ألفا (Cronback's Alpha) و ذلك باستخدام برنامج SPSS للاستمارة ككل كما يعرض الجدول(٣)

جدول (٣)

يوضح نتائج معامل الثبات والصدق للاستمارة ككل (١)

المتغير	الثبات	الصدق
قائمة الاستبيان	٠,٩٥٤	٠,٩٧٧

و يتضح من الجدول السابق أن معامل الثبات ذو درجة عالية يمكن الاعتماد عليها لقياس اتساق الإجابات بين المستقصي منهم ، حيث يعتبر مؤشر جيد التحليل لاستمارة الاستقصاء . و تم الحصول علي معامل الصدق بالحصول علي الجذر التربيعي لمعامل الثبات .

و بعد التحقق من توافر الثبات و الاستقرار، بالإضافة إلي صدق محتوي قائمة الاستقصاء إحصائيا فإنه يمكن التسليم إلي حد كبير بصحة البيانات التي تم الوصول إليها ، و من ثم يمكن تعميم النتائج التي يتم التوصل إليها علي المجتمع الأصلي للدراسة إذا توافرت نفس الظروف التي أجريت فيها هذه الدراسة .

٢- التحليل الوصفي لاستمارات الاستقصاء:-

لعرض البيانات جدوليا لتكون بصيغة مفهومه وذات مدلول يتعلق بالظاهرة محل الدراسة . وهذا الجزء يمثل الشق الوصفي الذي يتعامل مع البيانات الإحصائية التي حصلنا عليها من خلال استمارات الاستقصاء من عينة الدراسة دون التعميم.

و قام الباحث باستخدام أحد مقاييس النزعة المركزية وهو المتوسط الحسابي لمعرفة اتجاه ردود المستقصي منهم لكل عبارة إلي اتخاذ قيمة معينة تتركز حولها هذه الردود. وبالرغم من أهمية وفائدة المتوسط الحسابي إلا أنه لا يوضح بصورة كاملة طبيعة التوزيع . ومن ثم قام الباحث باستخدام الانحراف المعياري

[١] - ملاحق الدراسة (ملحق رقم ٢ مخرجات التحليل الإحصائي)

كأحد أهم مقاييس التشتت لمعرفة درجة انتشار قيم ردود المستقصي منهم حول المتوسط الحسابي .
ومن المعروف أنه عندما يكون التشتت صغيرا فإن المتوسط الحسابي يعبر عن القيمة النموذجية أي القيمة التي تمثل تقريبا مفردات القيم وأن المتوسط الحسابي في هذه الحالة يعتبر تقديرا مأمونا أي يمكن الاعتماد عليه أو أنه تقديرا جيدا للمتوسط في المجتمع . أما إذا كان التشتت كبيرا فإن المتوسط لا يمثل القيمة النموذجية وغير مأمونا أي لا يمكن الاعتماد عليه ما لم تكن العينة كبيرة جدا .

جدول (٤)

يعرض تحليلا لردود المستقصي منهم عن عبارات قائمة الاستقصاء

رمز	العبارة	المتوسط الحسابي	الانحراف المعياري
X1	**إجراءات تخفيف العمالة**		
X11	١- زيادة التهديدات الداخلية .	4.5856	.49485
X12	٢- تقليل فصل المهام .	4.6757	.47024
X13	٣- ضعف في عزل المعرفة للعاملين .	4.9369	.24418
X14	٤- إمكانية اختراق الأنظمة من جانب الموظفين	4.8108	.39344
X15	٥- زيادة التواطؤ بين العاملين لاختراق النظام من الداخل	4.8739	.33350
X2	**إجراءات الإغلاق**		
X21	١- زيادة التهديدات الخارجية .	4.8739	.33350
X22	٢- ضعف برامج وأنظمة التأمين المستخدمة من خلال الأجهزة الشخصية للعاملين بالبنك .	4.6757	.47024
X23	٣- وجود ثغرات تمكن الدخول لغير المرخص لهم بسهولة إلي أنظمة البنك .	4.9369	.24418
X24	٤- ضعف عملية الرقابة والمراجعة .	4.7477	.43627
X3	**المخاطر**		
X31	١- مخاطر الوصول أو الأمن	4.8739	.33350
X32	٢- مخاطر السلامة (التكامل)	4.9369	.24418
X33	٣- مخاطر الملاءمة	4.6757	.47024
X34	٤- مخاطر الإتاحة	4.9369	.24418
X35	٥- مخاطر البنية التحتية	4.5856	.49485
X36	٦- مخاطر استمرار تقديم الخدمات	4.9369	.24418
Y	**عناصر أمن المعلومات**		

Y1	١- التحقق من الهوية	4.6757	.47024
Y2	٢- التحكم بالوصول	4.9369	.24418
Y3	٣- السرية	4.8739	.33350
Y4	٤ - سلامة المعلومات وتكاملها	4.9369	.24418
Y5	٥- عدم الإنكار	4.5856	.49485
Y6	٦- توافر أو ديمومة المعلومة	4.6757	.47024
Y7	٧- المتابعة أو المراجعة	4.9369	.24418

و يتضح من البيانات الواردة بالجدول رقم (٤) أن : -

- المتوسط الحسابي لردود المستقصي منهم يتراوح قيمته بين (٤,٦٨ ، ٤,٩٤) وهذا يعني ارتفاع نسبة التكرارات لردود المستقصي منهم في عينة الدراسة بين " مؤثر تماما " و" مؤثر" .
- انخفاض الانحراف المعياري حيث يتراوح قيمته بين (٠,٢٤٤ ، ٠,٤٩٥) مما يدل علي اتفاق معظم المستقصي منهم علي تأثير الإجراءات الاحترازية علي الرقابة الداخلية والمخاطر التي يمكن أن تؤدي لها وأيضا عناصر أمن المعلومات .

٣- التحليل الإحصائي المتقدم : تم استخدام عدد من الأساليب الإحصائية لاختبار مدي صحة فروض الدراسة هي كما يلي :-

١/٣- اختبارات الفروق (تحليل التباين) ANOVA لاختبار مدي صحة الفرض الأول .

تحليل التباين هو الطريقة المستخدمة لاختبار فرض تساوي أكثر من متوسطين مقابل فرض عدم تساوي بعض هذه المتوسطات مع بعض (علي الأقل عدم تساوي متوسطين). ويعتمد تحليل التباين علي الاختبار الإحصائي " F " .

تحليل التباين (لاختبار مدي صحة الفرض الأول) : علي مستوي الفئات المستقصي منهم بالنسبة لتأثير الإجراءات الاحترازية علي الرقابة الداخلية والمخاطر التي يمكن أن تؤدي لها وأيضا عناصر أمن المعلومات في البنوك التجارية .

ويعرض الجدول رقم (٥) تحليل الفروق لمتوسط ردود المستجوبين علي مستوي الفئات المستقصي منهم لمتغيرات الدراسة .

جدول رقم (٥)
يعرض تحليل الفروق لمتوسط ردود المستجوبين للفئات المستقصي منهم لمتغيرات الدراسة

المتغيرات	F	المعنوية
(X1) إجراءات تحفيف العمالة	.012	.989
(X2) إجراءات الإغلاق	.052	.950
(X3) المخاطر	.021	.979
(Y) عناصر أمن المعلومات	.039	.961

عند مستوي المعنوية (٠,٠٥)

أوضحت نتائج تحليل استمارة الاستقصاء أنه لا يوجد فروق معنوية بين استجابات عينة الدارسة للمتغيرات الخاصة بتأثير الإجراءات الاحترازية علي الرقابة الداخلية والمخاطر التي يمكن أن تؤدي لها وأيضا عناصر أمن المعلومات في البنوك التجارية . ويرجع ذلك إلي عدم الاختلاف بين الفئات المستقصي منهم علي أهمية الرقابة الداخلية بالنسبة لأمن المعلومات في البنوك التجارية والمخاطر التي يمكن أن تتعرض لها في حال وجود نقاط ضعف في أنظمة الرقابة الداخلية في ظل تطبيق الإجراءات الاحترازية حال تفشي فيروس كورونا ، وأيضا عناصر أمن المعلومات .

و من خلال نتائج تحليل الفروق يلاحظ أنه يتم قبول الفرض العدمي الأول " لا توجد اختلافات ذات دلالة إحصائية بين متوسط آراء عينات الدراسة للبنوك الثلاثة علي انعكاسات تفشي فيروس كورونا علي نظم الرقابة الداخلية وأثرها علي أمن المعلومات بالبنوك التجارية " .

٢/٣- تحليل الارتباط Correlation لاختبار مدي صحة الفرض الثاني:-
لمعرفة وتقييم العلاقة بين متغيرات الدراسة ، ويوضح معامل الارتباط نوع و درجة العلاقة بين هذه المتغيرات .
وسوف نقوم بعرض مصفوفة برسون للارتباط بين متغيرات الدراسة كما بالجدول (٦) . و يتضح من خلال مصفوفة الارتباط وجود ارتباط طردي قوي بين متغيرات الدراسة[١] .

[١] - ملاحق الدراسة – ملحق رقم (٢)

جدول رقم (٦) يعرض مصفوفة الارتباط بين متغيرات الدراسة

		Y	X1	X2	X3
Y	R	١			
	المعنوية				
X1	R	.942**	١		
	المعنوية	.000			
X2	R	.932**	.923**	١	
	المعنوية	.000	.000		
X3	R	.907**	.971**	.832**	١
	المعنوية	.000	.000	.000	

**** عند مستوي المعنوية (٠,٠١)**

المتغير التابع (أمن المعلومات)

و يتضح من خلال مصفوفة الارتباط وجود ارتباط طردي قوي بين متغيرات الدراسة ، حيث يوجد ارتباط طردي قوي ومعنوي بين المتغير التابع أمن المعلومات وكل من المتغيرات المستقلة التالية (X1) إجراءات تخفيف العمالة ، (X2) إجراءات الإغلاق ،(X3) المخاطر المترتبة علي تطبيق الإجراءات الاحترازية .

وهذا يدل علي وجود علاقة ارتباط جوهرية بين أمن المعلومات بالبنوك التجارية وتطبيق الإجراءات الاحترازية والمخاطر المترتبة عليها في حالة تفشي فيروس كورونا ، مما يؤكد علي رفض الفرض العدمي الثاني : " لا يوجد علاقة ارتباط جوهرية بين انعكاسات تفشي فيروس كورونا علي نظم الرقابة الداخلية و أمن المعلومات بالبنوك التجارية " وقبول الفرض البديل .

٣/٣- الانحدار المرحلي Stepwise Regression لاختبار مدي صحة الفرض الثالث :-

و يستخدم تحليل الانحدار المرحلي في التنبؤ بتغيرات المتغير التابع الذي يؤثر فيه عدة متغيرات مستقلة . وقد تم اختيار طريقة Stepwise حيث يتم إدخال المتغيرات المستقلة إلي معادلة الانحدار علي خطوات ، والغرض منها هو تحديد أهم المتغيرات المستقلة المؤثرة علي المتغير التابع .

وكان من نتائج التحليل ما يلي :-

١- من خلال الجدول الأول بملاحق الدراسة [١] تبين أن أهم المتغيرات المستقلة المؤثرة علي المتغير التابع (أمن المعلومات) هي بالترتيب كما ورد بالجدول

[١] - ملاحق الدراسة (ملحق رقم ٢)

الأول بملاحق الدراسة ، المتغير الأول (X1) إجراءات تحفيف العمالة ، المتغير الثاني (X2) إجراءات الإغلاق ،المتغير الثالث (X3) المخاطر المرتبة علي تطبيق الإجراءات الاحترازية .

من خلال نتائج تحليل الارتباط و تحليل الانحدار المرحلي نجد أن التهديدات الداخلية الناتجة عن إجراءات التخفيف أكثر تأثيرا وارتباطا من التهديدات الخارجية الناتجة عن إجراءات الأغلاق ، وكليهما يؤدي إلي مجموعة من المخاطر تؤثر علي أمن المعلومات .

٢- يتضح من خلال الجدول الثاني - بملاحق الدراسة- من تحليل الانحدار المرحلي أن قيم معامل الارتباط البسيط المجمع للمتغيرات المستقلة الثلاثة المؤثرة علي المتغير التابع قد بلغ (٠,٩٦٤) بينما بلغ معامل التحديد R2 للمتغيرات الثالثة (٠,٩٢٩) وأيضا معامل التحديد المصحح (٠,٩٢٧) مما يعني أن المتغيرات التفسيرية الثلاثة استطاعت أن تفسر ٩٢,٧ % من التغيرات الحاصلة علي المتغير التابع والباقي ٧,٣ % يرجع إلي عوامل أخري . ويمكن توزيع نسب التفسير للمتغيرات المستقلة كما يلي : المتغير الأول بنسبة ٨٨,٥ % ، والمتغير الثاني بنسبة ٢,٧ % والمتغير الثالث ١,٥ % ، كما يتضح من الجدول رقم (٧) من خلال معامل التحديد المصحح .

جدول رقم (٧)

يعرض معامل الارتباط ومعامل التحديد للمتغيرات المستقلة المؤثرة علي المتغير التابع

المتغير	معامل الارتباط R	معامل التحديد R^2	معامل التحديد المصحح R^{-2}
(X1) إجراءات تخفيف العمالة	.942[a]	.886	.885
(X2) إجراءات الإغلاق	.956[b]	.913	.912
(X3) المخاطر	.964[c]	.929	.927

عند مستوي المعنوية (٠,٠٥)

٣ – الجدول الثالث بملاحق الدراسة يتضمن قيم تحليل التباين والذي يمكن من خلاله معرفة القوة التفسيرية للنموذج ككل عن طريق إحصائية F . و يتضح من جدول تحليل التباين المعنوية العالية لاختبار F (٠,٠٥ > P) حيث بلغت قيمة F(٤٦٣,٧٣٢) مما يؤكد القوة التفسيرية العالية للانحدار المرحلي من الناحية الإحصائية.

٤- الجدول الرابع من تحليل الانحدار المرحلي في ملاحق الدراسة [١] يعرض قيمة الثابت ومعاملات الانحدار ودلالتها الإحصائية للمتغيرات المستقلة المؤثرة علي المتغير التابع ويمكن تلخيص هذا الجدول في الجدول رقم (٨)

[١] - ملاحق الدراسة (ملحق رقم ٢)

جدول رقم (٨)
يعرض قيمة الثابت ومعاملات الانحدار ودلالتها الإحصائية للمتغيرات المستقلة المؤثرة علي المتغير التابع

المتغير	قيمة المعامل	قيمة اختبار T	المعنوية
الحد الثابت غير المعياري B	-.283-	-1.882-	.063
(X1) إجراءات تخفيف العمالة	-.509-	-2.092-	.039
(X2) إجراءات الإغلاق	.707	7.860	.000
(X3) المخاطر	.859	4.766	.000

عند مستوي المعنوية (٠,٠٥)
المتغير التابع (أمن المعلومات)

و يتضح من الجدول أن المتغيرات المستقلة الثلاثة معنوية في نموذج الانحدار المرحلي طبقا لاختبار T . كما يمكن التوصل إلي معادلة الانحدار المرحلي باستخدام Beta غير المعيارية (الحد الثابت) كما يلي :

أمن المعلومات بالبنوك التجارية = - ٠,٢٨٣ - ٠,٥٠٩ (إجراءات تخفيف العمالة) + ٠,٧٠٧ (إجراءات الإغلاق) + ٠,٨٥٩ (المخاطر المرتبة علي تطبيق الإجراءات الاحترازية) .

من نتائج تحليل الانحدار المرحلي السابق يلاحظ أنه يمكن رفض الفرض العدمي الرابع : " لا يوجد تأثير جوهري لانعكاسات تفشي فيروس كورونا لنظم الرقابة الداخلية علي أمن المعلومات بالبنوك التجارية " وقبول الفرض البديل .

نتائج الدراسة الميدانية :-

١- انتهت نتائج تحليل الفروق إلي قبول الفرض العدمي الأول " لا توجد اختلافات ذات دلالة إحصائية بين متوسط آراء عينات الدراسة للبنوك الثلاثة علي انعكاسات تفشي فيروس كورونا علي نظم الرقابة الداخلية وأثرها علي أمن المعلومات بالبنوك التجارية " .

٢- انتهت نتائج تحليل الارتباط إلي رفض الفرض النظري الثاني " لا يوجد علاقة ارتباط جوهرية بين انعكاسات تفشي فيروس كورونا علي نظم الرقابة الداخلية و أمن المعلومات بالبنوك التجارية " وقبول الفرض البديل .

٣- انتهت نتائج تحليل الانحدار المرحلي إلي رفض الفرض النظري الرابع " لا يوجد تأثير جوهري لانعكاسات تفشي فيروس كورونا لنظم الرقابة الداخلية علي أمن المعلومات بالبنوك التجارية " وقبول الفرض البديل .

التوصيات :

١- يجب علي الشركات المسئولة عن توفير أنظمة تكنولوجيا المعلومات بالبنك تزويد الأجهزة الشخصية للعاملين بالبنك وخاصة إدارة تكنولوجيا المعلومات

بأنظمة التشغيل عالية الكفاءة وتوفير برامج الحماية المناسبة وذلك للحد من اختراق أنظمة البنك من خلال تلك الأجهزة في حال استخدامها من المنازل في وقت الإغلاق .

٢- يجب عدم فتح الرسائل مجهولة الهوية وغير معروفة المصدر ، فقد تحتوي مرفقات البريد الإلكتروني علي فيروسات وديدان الحاسب الآلي ، وبرامج وأحصنة طروادة ، وبرامج الاختراق ، وبرامج التجسس الإلكتروني .

٣- تحديد مستوي النفاذ الصحيح لكل واحد من الموظفين ومستخدمي النظام ليقوموا بعملهم بدون السماح للجميع بالنفاذ الكامل لجميع الملفات والأنظمة .

٤- يجب تدريب الموظفين في إدارة تكنولوجيا المعلومات علي كيفية التعامل مع وسائل أمن المعلومات وخاصة في ظل جائحة كورونا ، حيث أن الجائحة سوف تستمر لأجل غير معروف .

٥- يجب إجراء عملية متابعة ومراجعة محاولات الدخول للنظام سواء كانت ناجحة أو فاشلة وتحديد الجهات التي تسعي للدخول إلي النظام .

٦- ضرورة أن يكون المراجع الداخلي أحد أعضاء فريق العمل الخاص بعملية إنشاء أو الحصول علي البرامج أو النظم الجديدة الخاصة بالبنك ، حيث إن محترفي تكنولوجيا المعلومات غالبا ما يكون لديهم فهم ضعيف عن ماهية عناصر الرقابة، ولماذا تكون مطلوبة. و يظهر هنا دور المراجعة في المساعدة في توجيه أفراد تكنولوجيا المعلومات عن أهمية عناصر الرقابة وذلك من خلال العمل سويا مع فريق عمل تكنولوجيا المعلومات و كذلك من خلال التدريب و ورش العمل .

٧- من خلال الواقع الميداني تبين أنه يجب علي البنوك اتلاف بطاقات الائتمان المنتهية (تثقيب البطاقات) حيث يقوم بعض الأشخاص في استخدامها للاستيلاء علي أموال الغير عن طريق استبدال البطاقات المنتهية بالبطاقات السليمة للأشخاص التي لا تعرف استخدام ماكينات الصراف الآلي بعد معرفة الرقم السري لهذه البطاقات من أصحابها .

المراجع

١-اتحاد المصارف العربية ، " أمن المعلومات : المخاطر وتحديات المستقبل " ، الأمانة العامة – إدارة الدراسات والبحوث ، ٩/٤/ ٢٠١٨.

٢-البنك المركزي المصري ، " الضوابط الرقابية للعمليات المصرفية الالكترونية وإصدار وسائل دفع لنقود الكترونية " ، البنك المركزي المصري ، ٢٨ فبراير ٢٠٠٢.

٣-البنك المركزي المصري ، " الضوابط الرقابية للعمليات المصرفية الالكترونية " ، البنك المركزي المصري ، ٢٠١٢ .

٤-اللجنة العربية للرقابة المصرفية " إدارة المخاطر التشغيلية و كيفية احتساب المتطلبات الرأسمالية لها " ، صندوق النقد العربي ، أبو ظبي ، سنة ٢٠٠٤.
٥-المعهد المصري للمحاسبين و المراجعين - معايير المراجعة،(القاهرة ، بدون سنة نشر).
٦-د/ إبراهيم الكراسنة ، " أطر أساسية ومعاصرة في الرقابة علي البنوك وإدارة المخاطر " ، صندوق النقد العربي – معهد السياسات الاقتصادية ، أبو ظبي ، مارس ٢٠٠٦.
٧-أ.د / أحمد حسين علي حسين " دليلك في : تحليل وتصميم النظم " ،الدار الجامعية – الإسكندرية ، سنة ٢٠٠٦.
٨-د/ السيد أحمد السقا ، وآخرون ، " الاتجاهات الحديثة في المراجعة المالية "، كلية التجارة – جامعة طنطا ، الطبعة الأولي ، ٢٠٠٥ .
٩-د/ أحمد عبد السلام أبو موسى ، " جرائم الكمبيوتر: هل يمكنك حماية نظام المعلومات المحاسبية الخاصة بك؟ " ، بحوث مؤتمر الاقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية، عمان، الأردن، ٢٠٠٢، ص ٦٠٩-٦٢٥.
١٠- د/أحمد عبد السلام أبو موسى ، "أهمية مخاطر المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المنشآت السعودية"، المجلة العلمية للتجارة والتمويل، كلية التجارة، جامعة طنطا، العدد الثاني، ٢٠٠٤.
١١- د/ الوليد أحمد طلحه ، " التداعيات الاقتصادية لفيروس كورونا المستجد علي الدول العربية " ، صندوق النقد العربي ، إبريل ٢٠٢٠ ، ص ٥ .
١٢- د/ ثناء القباني " الرقابة المحاسبية الداخلية في النظامين اليدوي و الإلكتروني " (دار الكتاب الجامعي ، الإسكندرية ، سنة ٢٠٠٣).
١٣- د/ ثناء القباني " دراسات في المراجعة – برامج عملية المراجعة – مراجعة مجالات بيئة تشغيل البيانات الكترونيا - مراجعة التجارة الالكترونية "، بدون ناشر ، كلية التجارة – جامعة المنوفية ٢٠٠٨/ ٢٠٠٩.
١٤- د. خالد بن سليمان الغثبر ، د.م. محمد عبدالله القحطاني ، " أمن المعلومات بلغة مسيرة " ، مركز التميز لأمن المعلومات ، جامعة الملك سعود ، ٢٠٠٩ .
١٥- د/ خالد بن سليمان الغثبر ، د/ سليمان بن عبد العزيز بن هيشة ، " الاصطياد الإلكتروني : الأساليب والإجراءات المضادة " ، مركز التميز لأمن المعلومات ، جامعة الملك سعود ، ٢٠٠٩.
١٦- د. ذيب بن عايض القحطاني ، " أمن المعلومات " ، المملكة العربية السعودية ، مدينة الملك عبد العزيز للعلوم والتقنية KACST ، الرياض ٢٠١٥ .
١٧- د/ رأفت رضوان ، " التجارة الإلكترونية " ، القاهرة : المنظمة العربية للتنمية الإدارية ، ١٩٩٩.
١٨- د/ رشا حمادة ، " أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية " ، مجلة جامعة دمشق الاقتصادية والقانونية – المجلد ٢٦ – العدد الاول ، ٢٠١٠ .
١٩- ريتشارد مانسفيلد " حيل وأساليب الهاكرز وطرق الوقاية منها " ، ترجمة الدكتور خالد العامري ، القاهرة : الهيئة المصرية العامة للكتاب ، ٢٠٠٦ .

٢٠- ستيفن أ. موسكو ف. مارك ج – سيمكن . ترجمة د/ كمال الدين سعيد " نظم المعلومات المحاسبية لاتخاذ القرارات "، المملكة العربية السعودية : جامعة الملك سعود ، كلية الاقتصاد والإدارة فرع القصيم .
٢١- د/ سناء الدين فوزي ، وآخرون ، " أساسيات مراجعة الحسابات "، كلية التجارة – جامعة طنطا ، الطبعة الأولي ٢٠٠٢ .
٢٢- أ.د/ شوقي فوده ، دينا الدسوقي ، " أثر العلاقة بين فاعلية أمن نظم المعلومات المحاسبية الإلكترونية وربحية البنوك التجارية المصرية مع دراسة تطبيقية " ، مجلة الدراسات التجارية المعاصرة ، كلية التجارة – جامعة كفر الشيخ ، العدد السابع يونيو ٢٠١٩.
٢٣- أ.د. صدام محمد محمود ، أ.د .علي إبراهيم حسن ، " تداعيات الأزمات والنوازل المجتمعية علي الممارسات المحاسبية فيروس كورونا (COVID-19) أنموذجا دراسة نظرية تحليلية " ، جامعة تكريت ، كلية الإدارة والاقتصاد ، مجلة تكريت للعلوم الإدارية والاقتصادية ، المجلد (١٦) العدد (٤٩) ج١ ، ٢٠٢٠.
٢٤- د/ صلاح الدين الهيتي ، د/ أمنة ماجد الربيحات ، "أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية: دراسة ميدانية في عدد من الوزارات الأردنية وأمانة عمان الكبرى"، مجلة المحاسبة والإدارة والتأمين، جهاز الدراسات العليا والبحوث، كلية التجارة، جامعة القاهرة، العدد ٦٥، ٢٠٠٥ .
٢٥- د/ عطا الله أحمد الحسبان ، " مدي تعامل مدققي أنظمة تكنولوجيا المعلومات بمعايير التدقيق الخاصة ببيئة أنظمة المعلومات للمحافظة علي أمن وسرية المعلومات في البنوك الأردنية " ، مجلة كلية بغداد للعلوم الاقتصادية الجامعة – العدد العشرون – أ ، ٢٠٠٩ .
٢٦- أ.م. علي مال الله عبد الله ، د. خالص حسن الناصر ، " حوكمة أمن المعلومات ودورها في تخفيض مخاطر نظم المعلومات المحاسبية الالكترونية " ، " ورقة عمل مقدمة الى الندوة العلمية لقسم إدارة الاعمال كلية الإدارة والاقتصاد جامعة الموصل بالتعاون مع قيادة عمليات نينوى الموسومة" الإدارة الأمنية في محافظة نينوى " وسبل تطويرها " ، ديسمبر ٢٠١٩.
٢٧- د/ محمد محمد إبراهيم منصور ، " تأثير التجارة الالكترونية علي تصميم نظم المعلومات المحاسبية – إطار مقترح - " ، مؤتمر التجارة الالكترونية الآفاق والتحديات ، كلية التجارة جامعة الإسكندرية، المجلد الأول ، الإسكندرية ٢٥- ٢٧ يوليو٢٠٠٢ .
٢٨- د / محمد سامي راضي ،" المراجعة المتقدمة "، بدون ناشر، طنطا: كلية التجارة – جامعة طنطا، سنة ٢٠٠٠.
٢٩- منال صبحى على البلقاسى ،" أثر تطبيق حوكمة تكنولوجيا المعلومات وفقا لـ 5 Cobit على مخاطر نظم المعلومات الالكترونية : دراسة ميدانية على المعاهد العالية الخاصة " ، المجلة المصرية للدراسات التجارية ، كلية التجارة - جامعة المنصورة ، مجلد ٤٢ ، العدد الأول ٢٠١٨ .
٣٠- د/ نزار إبراهيم قويدر ، (نظم الرقابة الداخلية وأثرها علي أمن المعلومات " دراسة ميدانية علي شركة المدار للهاتف المحمول ") ، المجلة الجامعة - كلية

1- Abu-Musa, Ahmad A. (2010), "Information security Governance in Saudi Organization: An Empirical Study " Pubic Administration, A Professional Quarterly Journal Published by the Institute of Public Administration Riyadh, Saudi Arabia.
2- Al-Hanini, Eman (2012), " The Risks of Using Computerized Accounting In-formation Systems in the Jordanian Banks: Their Reasons and Ways of Pre-vention", European Journal of Business and Management, Vol. 4, No. 20 .
3- Alvin A. Arens , Randal J. Elder , Mark S. Beasley ," Auditing and Assurance Services ,12th Edition ", New Jersey , Prentice Hall , 2008.
4- Bhaskar, S. M., and Ahson S. I., "Information Security: A practical Approach", Alpha Science International LTD, Oxford, U.K., 2008 .
5- D.H. Taylor and W.G.،Glezen ، " Auditing Integrated Concepts and Procedures " ، (N.Y. ، John Wiley & Sons ، Inc. ، 1991).
6- Information Systems Audit and Control Association (ISACA), "COBIT 4.1 Framework for IT Governance and Control", Available at: www.isaca.org, Accessed: 25 May, 2014.
7- Henning Hagerman , William Kinney , Karlheinz Kuting , Claus-Peter Weber ," Internal Audit Handbook Management with the SAP-® Audit Roadmap ", German : Acid-free paper ,2008.
8- IT Governance Institute," IT Control Objectives For Sarbanes-Oxley ", IT Governance Institute ,USA , 2004.
9- IT Governance Institute ,"COPIT 4.1 Excerpt - Executive Summary Framework ", IT Governance Institute, USA , 2007 , P 15 . http://www.ITgi.org
10- IT Governance Institute, "IT Control Objectives for Sarbanes-Oxley", IT Governance Institute , 2004 .
11- IT Governance Institute ,"Enterprise Risk : Identify, Govern and Manage IT Risk – The Risk IT Framework " , IT Governance Institute ,USA , 2009 .
12- Jack E. Kiger & James H . Scheiner ," Auditing ", New Jersey , Houghton Mifflin Company , 1994 .

13- Kris Seeburn ," COBIT as an It Governance Mechanism ", IT Governance Institute 2008 and ISACA Serving IT Governance Professionals.
14- Kankanhalli, Atreyi et al., "An Integrative Study of Information Systems Security effectiveness," International Journal of Information Management, Vol. 23, (2003) .
15- McDaniel, George(1994), "IBM Dictionary of Computing", McGraw-Hill, Inc , New York, 1994.
16- Mangard et. Al., "Power Analysis Attacks: Revealing the Secrets of Smart Cards", Springer Science and Business Media, LCC, 2007.
17- Mario Spremic ," IT Governance and IT Risk Management for Supporting ' Always-on ' Enterprise Information Systems" , IGI Global , 2010.
18- Rosslin John Robles , and others , " SOX and Its effects on IT security Governance " , International Journal of Smart Home , Vol.3,No.1, January ,2009.
19- R . Weber ," EDP Auditing :Conceptual Foundations and Practice " , London: McGraw - Hill Book Company , 1988 .
20- Stallings, William (2007), "Network Security Essentials: Applications and Standards", Third Edition, Prentice-Hall, 2007.
21- Stallings, William (2006), "Cryptography and Network Security: Principles and Practices", Fourth Edition, Prentice-Hall, 2006.
22- T. Olzak, (2013), "COBIT 5 for Information Security: The Underlying Principles",www.techrepublic.com View publication
23- The National Computing Centre ,"IT Governance : Developing a successful governance strategy", National Computing Centre (NCC) , 2005.
24- The Committee on National Security Systems: http://www.cnss.gov
25- The Institute Of Internal Auditors, " Sarbanes – Oxley Section 404 : A Guide for Management by Internal Controls Practitioners ", AII,2nd Edition, January 2008.www.theiia.org .
26- The Institute Of Internal Auditors (IIA) , " International Standards for the Professional Practice of Internal Auditing " , USA ,Florida , 2010.

27- **Walter G. Kell and William C. Boynton ، " Modern Auditing " (New York : John Wiley & Sons ، Inc.، 1992) .**

28- **Withman, M. and Mattord, H.(2005), "Principles of Information Security", Second Edition, Thomson Course Technology, 2005.**

ملاحق الدراسة

ملحق رقم (١) قائمة الاستقصاء

المتغير	مؤثر تماما	مؤثر	مؤثر إلي حد ما	غير مؤثر	غير مؤثر تماما
أولا : يمكن أن تؤدي إجراءات تخفيف العمالة في إدارة تكنولوجيا المعلومات بالبنك في ظل تفشي فيروس كورونا إلي :					
١ - زيادة التهديدات الداخلية .					
٢ - تقليل فصل المهام .					
٣ - ضعف في عزل المعرفة للعاملين .					
٤ - إمكانية اختراق الأنظمة من جانب الموظفين					
٥ - زيادة التواطؤ بين العاملين لاختراق النظام من الداخل					
ثانيا : يمكن أن يؤدي إجراءات الإغلاق في إدارة تكنولوجيا المعلومات بالبنك في ظل تفشي فيروس كورونا إلي :					
١ - زيادة التهديدات الخارجية .					
٢ - ضعف برامج وأنظمة التأمين المستخدمة من خلال الأجهزة الشخصية للعاملين بالبنك .					
٣ - وجود ثغرات يمكن الدخول غير المرخص لهم بسهولة إلي أنظمة البنك .					
٤ - ضعف عملية الرقابة والمراجعة .					
ثالثا : المخاطر التي يمكن أن تتزايد بسبب اتباع الإجراءات الاحترازية في ظل تفشي فيروس كورونا إلي :					
١ - مخاطر الوصول أو الأمن					
٢ - مخاطر السلامة (التكامل)					
٣ - مخاطر الملاءمة					
٤ - مخاطر الإتاحة					
٥ - مخاطر البنية التحتية					
٦ - مخاطر استمرار تقديم الخدمات					
رابعا : ماهي عناصر أمن المعلومات التي يمكن أن تتأثر في حال تطبيق الإجراءات الاحترازية في ظل تفشي فيروس كورونا ؟					
١ - التحقق من الهوية					
٢ - التحكم بالوصول					
٣ - السرية					
٤ - سلامة المعلومات وتكاملها					
٥ - عدم الإنكار					
٦ - توافر أو ديمومة المعلومة					
٧ - المتابعة أو المراجعة					

ملحق رقم (٢) مخرجات SPSS

Reliability
Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	111	100.0
	Excluded[a]	0	.0
	Total	111	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.954	22

Descriptives

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
X11	111	4.00	5.00	4.5856	.49485
X12	111	4.00	5.00	4.6757	.47024
X13	111	4.00	5.00	4.9369	.24418
X14	111	4.00	5.00	4.8108	.39344
X15	111	4.00	5.00	4.8739	.33350
X21	111	4.00	5.00	4.8739	.33350
X22	111	4.00	5.00	4.6757	.47024
X23	111	4.00	5.00	4.9369	.24418
X24	111	4.00	5.00	4.7477	.43627
X31	111	4.00	5.00	4.8739	.33350
X32	111	4.00	5.00	4.9369	.24418
X33	111	4.00	5.00	4.6757	.47024
X34	111	4.00	5.00	4.9369	.24418
X35	111	4.00	5.00	4.5856	.49485
x36	111	4.00	5.00	4.9369	.24418
Y1	111	4.00	5.00	4.6757	.47024
Y2	111	4.00	5.00	4.9369	.24418
Y3	111	4.00	5.00	4.8739	.33350
Y4	111	4.00	5.00	4.9369	.24418
Y5	111	4.00	5.00	4.5856	.49485
Y6	111	4.00	5.00	4.6757	.47024
Y7	111	4.00	5.00	4.9369	.24418
Valid N (listwise)	111				

ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.002	2	.001	.012	.989
Within Groups	8.457	108	.078		
Total	8.459	110			
Between Groups	.011	2	.005	.052	.950
Within Groups	11.380	108	.105		
Total	11.391	110			
Between Groups	.003	2	.001	.021	.979
Within Groups	7.397	108	.068		
Total	7.400	110			
Between Groups	.007	2	.004	.039	.961
Within Groups	10.078	108	.093		
Total	10.086	110			

Correlations

Correlations

		Y	X1	X2	X3
Y	Pearson Correlation	1	.942**	.932**	.907**
	Sig. (2-tailed)		.000	.000	.000
	N	111	111	111	111
X1	Pearson Correlation	.942**	1	.923**	.971**
	Sig. (2-tailed)	.000		.000	.000
	N	111	111	111	111
X2	Pearson Correlation	.932**	.923**	1	.832**
	Sig. (2-tailed)	.000	.000		.000
	N	111	111	111	111
X3	Pearson Correlation	.907**	.971**	.832**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	111	111	111	111

**. Correlation is significant at the 0.01 level (2-tailed).

Regression

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	X1	.	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).
2	X2	.	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).
3	X3	.	Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).

a. Dependent Variable: Y

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.942[a]	.886	.885	.10250
2	.956[b]	.913	.912	.08992
3	.964[c]	.929	.927	.08205

a. Predictors: (Constant), X1

b. Predictors: (Constant), X1, X2

c. Predictors: (Constant), X1, X2, X3

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.940	1	8.940	850.915	.000[b]
	Residual	1.145	109	.011		
	Total	10.086	110			
2	Regression	9.212	2	4.606	569.693	.000[c]
	Residual	.873	108	.008		
	Total	10.086	110			
3	Regression	9.365	3	3.122	463.732	.000[d]
	Residual	.720	107	.007		
	Total	10.086	110			

a. Dependent Variable: Y

b. Predictors: (Constant), X1

c. Predictors: (Constant), X1, X2

d. Predictors: (Constant), X1, X2, X3

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.104-	.169		-.618-	.538
	X1	1.028	.035	.942	29.170	.000
2	(Constant)	.020	.149		.134	.894
	X1	.597	.081	.547	7.415	.000
	X2	.402	.069	.428	5.800	.000
3	(Constant)	-.283-	.150		-1.882-	.063
	X1	-.509-	.243	-.466-	-2.092-	.039
	X2	.707	.090	.751	7.860	.000
	X3	.859	.180	.735	4.766	.000

a. Dependent Variable: Y

Excluded Variables[a]

Model		Beta In	t	Sig.	Partial Correlation	Collinearity Statistics
						Tolerance
1	X2	.428[b]	5.800	.000	.487	.147
	X3	-.126-[b]	-.927-	.356	-.089-	.057
2	X3	.735[c]	4.766	.000	.418	.028

a. Dependent Variable: Y

b. Predictors in the Model: (Constant), X1