حماية أمن انظمة المعلومات
دراسة حالة في مصرف الرافدين / فرع شارع فلسطين

م. م ندى اسماعيل جبوري
كلية الادارة والاقتصاد / جامعة بغداد

المستخلص:

اصبحت ادارة أمن انظمة المعلومات قضية حاسمة لاي منظمة في عصر المعلوماتية وكأي عملية اخرى لايمكن ادارة أمن المعلومات من غير مقياس قابل للقياس ، اذ يعد هذا الموضوع مهم في الوقت الذي تكون فيه المنظمات تحت ضغوط معقدة تتطلب المثابرة لحماية اصول بياناتهم المهمة . فالمقياس المعياري Common Vulnerability Scoring System (cvss) (نظام التنبيه وتسجيل المخاطر) سيؤهل المنظمات للتعرف مسبقاً على التهديدات ونقاط الضعف والمخاطر الموجودة لديهم . اذ يسعى البحث من خلال ذلك الى تحليل مؤشرات امنية انظمة المعلومات لمنع المخاطر والاختراقات المحتملة من خلال اعتماد المقياس المعياري (CVSS).

اجريت الدراسة في (مصرف الرافدين / فرع شلرع فلسطين) وذلك باستعمال قائمة الفحص (checklist) بوصفها اداة جمع المعلومات فضلاً عن المعايشة الميدانية للباحث اذ آلت المعلومات لتتحول بفعل الادوات الاحصائية الى نتائج وتوصيات شخصت واقع وسير العملية البحثية والعلاقات الحقيقية بين تلك المؤشرات التي تتعلق بالمعايير المؤقتة والبيئية ، اذ صيغت مشكلة الدراسة بعدد من التساؤلات تمثلت في الخوض بامكانية الاستفادة من تطبيق قياسات منع الاختراق والمحافظة على السرية ، كما هدفت الدراسة الى تحليل العلاقة بين مؤشرات ومعاملات الدراسة في المصرف عينة البحث وامكانية تطبيقه.

Saving the security of the information systems
A field Study in Bank of Rafidain / the branch Palestine Street

Abstract

The administration of the security of informational systems became a significant case to any system in the age of information's, as any other operation the administration of the security of information's can not be done without a measurable criteria, this subject is important in the time the organizations are under complex pressures need to work hard to secure their important organs. The measurable criteria (CVSS) ; the System of alarming when being attacked and risks will enable the organizations to face the threats and their weak points and risks in advance . The paper aims, through this, to analyze the security marks of informational system to prevent the risks and probable intruding through depending an the measurable criteria (cvss). (Rafidain Bank / Palestine Street) has been chosen the study to diagnose the research's operation and the real relations between these marks which are concerned with the commemoratory criteria's and environment in order to reach to a group of conclusions and recommendations that cooperate developing and keeping the security and secret of the information system of the research bank.

The study has been done in (the Rafiden Bank/ Palestine street branch) by using the checklist , as it is a tool for collecting information which trans formed by the statistical tools to results and recommendations. It diagnosed the process of the operation of the research and the red relations between these marks which are associated with the environment temporary criteria's as the problem of the study been forced out of number of questions represented by setting out the ability of taking benefit of the applying measures of preventing the intruding and to keep the secrecy . the study also aims to analyze the relation between the study's marks in the model bank of this study and the ability of applying .

المقدمة :

تلعب نظم المعلومات دوراً كبيراً في منظمات الاعمال كونها توفر المعلومات الضرورية لها فيما يخص الاسواق والمنافسين فضلاً عن معلومات البيئتين الداخلية والخارجية وما يتعلق بالوظائف الادارية وتتعرض نظم المعلومات الى مخاطر كبيرة لذلك ينبغي على المنظمات حمايتها والرقابة عليها لضمان سرية المعلومات الخاصة بها اذ تختلف اساليب الحماية باختلاف الاضرار ومصادرها لذا اتبعت وتتبع المنظمات اساليب وطرائق عديدة لحماية انظمة معلوماتها .

اذ تدور الرؤية الفكرية للدراسة الحالية حول ماهية أمنية نظم المعلومات والذي هي عبارة عن مجموعة الاجراءات والتدابير الوقائية التي تستخدم للحفاظ على سرية وحماية المعلومات فضلاً عن معرفة عناصره الاساسية وكيفية قياس أمن انظمة المعلومات وتوضيح الطرائق الثلاث الذي من خلالها يمكن الوصول لنظام تسجيل المخاطر (المقياس المعياري) (cvss) والى معاملات مقاييس المخاطر ومقاييس تقييم اداء المخاطر فضلاً عن معاملات نظام التنبيه للمخاطر .

استعمل منهج دراسة الحالة (case study) منهجاً للبحث ، كما جرى منها متضمنات الدراسة في أربع مباحث ، تناول المبحث الاول تحديد المشكلة والاهمية والاهداف ومعرفة الفرضية الرئيسة للبحث فيما تناول المبحث الثاني التعرف على المفاهيم المتعلقة بأمن انظمة المعلومات والمخاطر التي يواجهها وكيفية الحماية من تلك المخاطر ، فيما تكفل المبحث الثالث بعرض وتحليل المعالجة الاحصائية وتبني المقياس واختتمت الدراسة بمبحث اخير ضم الاستنتاجات والتوصيات والتي من ابرزها انخفاض القيام بكشف المخاطر بالسرعة المطلوبة مما يستدعي قيام المصرف المبحوث بتعزيز استخدام الوسائل التي تؤدي الى توافر نظام المخاطر المتعلقة بالوقت ، ومن بين اهم التوصيات للمصرف عينة البحث ان يعمل جاداً للاستفادة القصوى من استخدام مقياس الأمن المعياري وتطبيقه لحماية انظمة معلومات المصرف .

المبحث الاول/ منهجية الدراسة

١-١ : مشكلة الدراسة : تتمحور مشكلة البحث في ايجاد المنظمات لطرائق مختلفة تتمثل في مواجهة بيئة العمل العراقية من محدودية تطبيق انظمة المعلومات وايجاد مؤشرات حقيقية لتقيس أمنية أنظمة المعلومات تلك ، كما تاكد ذلك من المعايشة الميدانية لمصرف الرافدين/ فرع شارع فلسطين اذ يفتقر لمقاييس واقعية وحقيقية لأمنية المعلومات. وعليه يمكن تحديد المشكلة من خلال التساؤلات الاتية:-

١- هل يمكن تطبيق نظام التنبيه عند التعرض للمخاطر المحتملة (CVSS) .

٢- هل يمكن الاستفادة من تطبيق قياسات منع الاختراق والمحافظة على السرية في استخدام انظمة المعلومات .

٣- ماهي طبيعة العلاقات بين مؤشرات المقياس من اجل تحسين وتطبيق نظام أمني للمصرف .

١-١ - ٢ : أهداف البحث :يسعى البحث الى تحقيق الاهداف الاتية :-

١- عرض وتحليل واقع ومؤشرات المقاييس الامنية لمنع اختراق انظمة معلومات المصرف المبحوث .

٢- تحليل العلاقات فيما بين مؤشرات أمن انظمة المعلومات وطبيعة ارتباطها بالقياسات الامنية لتشخيص مستويات الدقة في توفير الحماية والأمن لها .

١- ١ - ٣ : أهمية البحث : تكمن اهمية البحث من خلال مواكبة التقدم العلمي الهائل الذي يحتاج اليه العالم اليوم ، اذ ان تقدم الشعوب يقترن بالتقدم العلمي والتقني في مجال الاتصال ونظم المعلومات والحاسوب ، لذا اصبح من الضروري حفاظ المنظمات على سرية اعمالها من

خلال استخدام مقاييس أمنية معينة لمنع اختراق انظمة معلوماتها والحد من الحوادث الامنية في اختراق االمعلومات .

١- ١- ٤ : فرضية الدراسة:اتساقا" مع مشكلة واهداف البحث صيغت الفرضيات الاساسية الاتية :

١- يتوقع تحسين أمن وحماية نظام المعلومات في المصرف المبحوث عند وجود علاقات ارتباط بين مؤشرات مقياس أمن نظام التنبيه للمخاطر ومعاملاته.

٢- يتوقع ان استخدام مقاييس المخاطر يساعد في السيطرة على فرض أمنية المعلومات وتقليل المخاطر .

٣- يتوقع من تقييم الادارة العليا للاداء انها تستطيع تحليل متطلبات أمن المعلومات والمساهمة والقدرة في تحديد المخاطر .

١- ١- ٥ : اساليب جمع البيانات وتحليلها :بهدف الحصول على البيانات اللازمة التي تساعد في تنفيذ اهداف البحث والوصول الى النتائج المطلوبة

اعتمدت الباحث في جمع البيانات والمعلومات على جانبين اساسيين هما :-

١- **الجانب النظري** :- فقد تم اثراء الجانب النظري من هذه الدراسة بالرجوع الى المصادر العلمية من كتب ومجلات وبحوث عربية واجنبية ومواقع تصفح على شبكة الويب مما ساعد الباحث على الالمام وتأطير الافكار المطلوبة لهذا المفهوم الحديث .

٢- الجانب التطبيقي :- اعتمدت الباحث على :

أ- المقابلات التي اجرتها الباحث مع اختصاصيي انظمة المعلومات في المصرف المبحوث والمسؤولين والعاملين فيه على اختلاف مهاراتهم وخبراتهم ، اذ تم ملئ استمارة الفحص من قبل الخبراء قي المصرف والذي بلغ عددهم (١٢) فضلاً عن ملئ الاستمارة من قبل الباحث نفسه من خلال معايشته وتحليله للحالة.

ب- المعايشة الميدانية لسير العمل من خلال استخدام تقنيات انظمة المعلومات في مصرف الرافدين / فرع شارع فلسطين.

ج- اعتمدت الباحث مقياس معتمد عالميا" (CVSS) نظام التنبيه عند التعرض للمخاطر وتسجيلها اذ بالامكان احتسابه بطريقة كمية على وفق معادلات من اجل قياس درجة تسجيل التعرض للخطر ومدى التنبيه له من خلال تطبيق المعادلات الرياضية الاتية والتي تم ايضاح رموزها في الملحق رقم (٢) : (doomun , 2009 : 854)

$$\mathbf{BS} = (10 \times AV \times AC \times A \times ((CI \times CIIB) + (II \times IIIB) + (AI \times AIB)$$

$$\mathbf{TS} = (BS \times RL \times E \times RC)$$

$$\mathbf{ES} = ((TS + (10 - TS) \times (CDP) \times TD))$$

$$\mathbf{CVSS} = BS \times TS \times ES$$

نظام التنبيه عند التعرض للخطر CVSS

المعاملات والمعايير المتعلقة بالمقياس وهي :-

١- النتيجة الاساسية BS (Base Score)

٢- قياس المعايير المؤقتةTS (Temporal Score)

٣- قياس المعايير البيئية ES (Environmental Score)

وقياس معاملات نظام التنبيه عند التعرض للخطر وهي : (CI, II, AI, A, AC, AV ، IB)

١- متجه الوصول للمعلومة AV = (Access Vector)

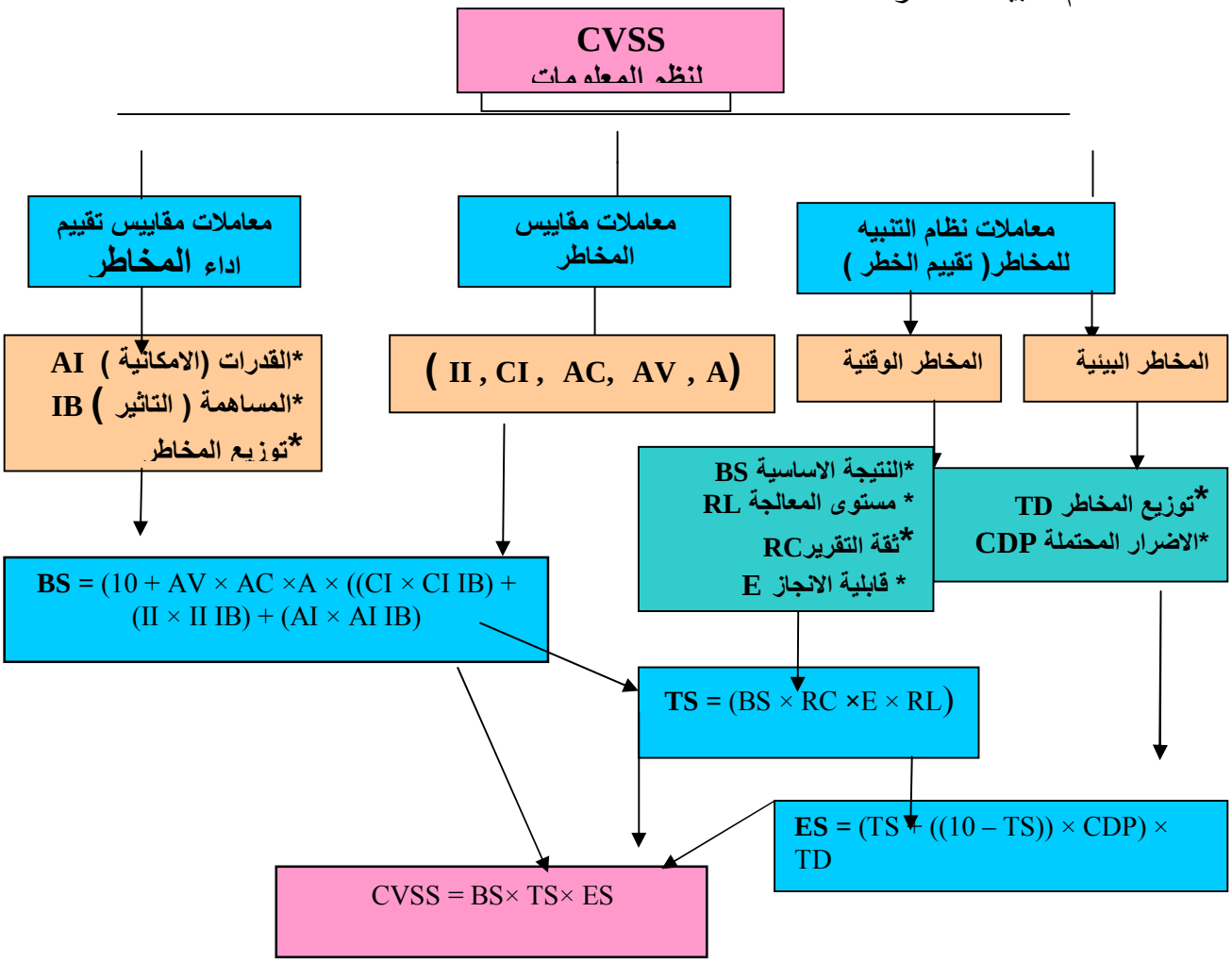
٢- تعقيد الوصول للمعلومة AC = (Access Complexity)

٣- المصداقية والتوثيق A = (Authentication)

٤- تأثير الامكانية (القدرة) AI = Availability Impact

٥- تأثير السلامة Integrity Impact = II
٦- قاعدة التأثير Confidentiality bias = IB
٧- تأثير السرية Confidentiality Impact = CI
د- استخدام المعالجات الاحصائية (ارتباط بيرسون ، النسب المئوية ، المتوسط الموزون)

١-١-٦ : انمـوذج البحـث: يمثـل انمـوذج البحـث النظـام الخـاص بالتنبيـه عنـد التعـرض للمخاطروتسجيلها اذ يشمل مقاييس تقييم اداء المخاطر، معاملات مقاييس المخاطر ومعاملات نظام التنبيه للمخاطر.



شكل (١) الصيغة الاساسية لنظام التسجيل الشامل للمخاطر

المصدر : من اعداد الباحثة

المبحث الثاني/الاطار النظري

اولاً / أمن نظم المعلومات

يتناول هذا المبحث التطرق لمتغيرات البحث الرئيسة للتعرف على المفاهيم والمنطلقات النظرية التي تساهم في الاجابة على تساؤلات وفرضية البحث وتحقيق الاهداف المتوخاة منه وكالاتي :-

١- <u>مفهوم أمن انظمة المعلومات</u>

سيتم تناول المفهوم والمخاطر والحماية لانظمة المعلومات فضلا" عن عناصره الاساسية والاطار العام لنظام تسجيل المخاطر اذ تشكل المعلومات للمنظمات البنية التحتية التي تمكنها من إداء مهامها اذ ان نوع المعلومات وكميتها وطريقة عرضها تعتبر الاساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة وعليه لابد من معرفة ما **الأمن** : اذ انه يشير الى السياسات والاجراءات والقياسات الفنية المستخدمة لمنع الوصول غير المخول او التغيير ا السرقة او الضرر المادي لنظم المعلومات (Laudon & Laudon , 2005 : 524)

ويرى (Doomun , 2009 : 851) ان الأمن هو ذات اهمية قصوى اذ ينبغي على المنظمة خدمة العديد من المنافسين والمستهلكين المباشرين والذي يعني الحفاظ على السرية التامة حول ارسال المعلومات لهم .

اما **أمن المعلومات** فانه يعد مجموعة الاجراءات والتدابيرالوقائية التي تستخدم سواء في المجال التقني او الوقائي للحفاظ على المعلومات والاجهزة والبرمجيات فضلاً عن الاجراءات المتعلقة بالحفاظ على العاملين في هذا المجال (Warman , 1993 : 12)

اما **أمن نظام المعلومات** فيقصد به الاليات التي تحمي مخازن المعلومات ومن ثم تمكن من تنفيذ الأمن (Ruth , et. al., 2009: 213) واشار (Swanson ,et. al., ٢٠٠٦ : 5) ان أمن نظام المعلومات :هو عملية الحماية من الاخطار والفيروسات التي قد تصيب انظمة المعلومات اذ يتطلب ذلك الوقت والجهد والموارد المالية لغرض الكشف عن المشاكل بالسرعة الممكنة والمساعدة في اتخاذ اللازم من طرق الحماية والمعالجة .

ويؤكد (Doomun , 2009 : 849) ان أمن انظمة المعلومات هو جزء مكمل لكل انشطة المنظمة المؤتمتة والذي قد تتعرض للمخاطر المحتملة ، إذ ان امن نظام المعلومات يشمل امن البيانات والمعلومات المخزونة وتخطيط التخلص من الخروقات الامنية .

واشار (O'Brien , 2001 : 448) ان امن نظام المعلومات يعد العلم الذي يبحث في االنظريات واستراتيجيات توفير الحماية للمعلومات والانظمة من المخاطر التي تهددها ومن انشطة الاعتداء عليها .

وتأسيسا" على ما سبق فان امن نظام المعلومات هو القدرة على االتفاعل وحماية المعلومات وقواعد البيانات من العبث والتدمير والكشف عن اي مخاطر تتعرض لها ومحاولة معالجتها بالسرعة والدقة الممكنتين ويعد من السياسات الامنية التي لابد للمنظمة من ان تتبناها من خلال افضل الممارسات الامنية واحدث التقنيات للحفاظ عليها من الاختراق غير المباشر من قبل غير المخولين ومهاجمة البيانات والمعلومات المخزونة في الحاسوب للضرربالمنظمة.

٢- <u>المخاطر التي تواجه أمن انظمة المعلومات</u>

تكون الانواع الكبيرة من البيانات عند خزنها بشكل الكتروني عرضة لانواع جديدة من التهديدات اكثر مما لو كانت موجودة بشكل يدوي فالاتصالات المتقدمة وبرامجيات الحاسوب كانت قد وسعت من هذا التعرض للخطر.إذ يمكن ربط نظم المعلومات في مواقع مختلفة من خلال شبكات الاتصالات ، والامكانية للوصول غير المخول او سوء الاستخدام او الاحتيال اذ انها غير محدودة بموقع واحد ولكن يمكن ان تحدث في اي نقطة وصول في الشبكة . فضلا" عن ذلك تكون المكونات المادية والبرمجيات وتنظيمات الافراد مطلوبة لشبكات الاتصالات مكونة بذلك مجالات وفرص جديدة للاختراق والاستخدام . ووفقاً لذلك يمكن تصنيف الاخطار المحتملة التي يمكن ان تتعرض لها نظم المعلومات بالاتي :-

أ- الاخطار البشرية : وهي التي يمكن ان تحدث خلال تصميم التجهيزات او نظم المعلومات او اثناء عمليات البرمجة او الاختبار او التجميع للبيانات واثناء ادخالها الى النظام ، او في عمليات تحديد الصلاحيات للمستخدمين ، وتشكل هذه الاخطار الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة نظم المعلومات في المنظمة (Laudon & Laudon , 2005 : 174)

ب- الاخطار البيئية : تشمل الزلازل والعواصف والفيضانات والاعاصير والمشاكل المتعلقة باعطال التيار الكهربائي والحرائق فضلا" عن المشاكل القائمة في تعطل انظمة التكييف واالتبريد وغيرها ودرجات الحرارة والرطوبة كلها تؤدي الى توقف هذه التجهيزات لفترات طويلة نسبياً لاجراء الاصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات (Swanson , et .al ., 2006: 17) .

ج- الجرائم المحوسبة : تمثل تحدياً كبيراً لادارة نظم المعلومات لما تسببه من خسارة كبيرة من خلال الاستخدام والوصول ، التعديل ، التدمير غير المفوض للماديات والبرامجيات او البيانات والموارد الشبكية ، فضلاً عن النشر والنسخ غير المفوض للمعلومات وحرمان المستفيد النهائي من الوصول الى ماديانه وبرامجياته او بياناته . وقد تكون جريمة الحاسوب بريئة نسبيا" مثل الاستخدام غير المفوض للحاسبات لاغراض شخصية ، او تكون خطرة كاستخدام الحاسبات لارسال موجودات المنظمة الحالية لحساب منظمات اخرى ومنها الاتي : (O'Brien , ٢٠٠٣382)

(أولاً) / فايروسات الحاسوب :

وهي عبارة عن برامج مستقلة تقوم بتحميل نفسها ضمن برمجيات الحاسوب ونسخ نفسها بشكل متكرر وبدون معرفة المستفيد والعديد من هذه الفايروسات يمكن ان تنتشر من نظام لاخر او تستقر في ذاكرة نظام ما وتقوم بتدمير برامج وبيانات معينة (Laudon & Laudon , 2005 : 525).

(ثانياً) / القرصنة : اي اختراق الاجهزة بدون عناء وبمجرد انزال احدى برامج القرصنة اذ المقصود بالقرصنة هو سرقة المعلومات من برامج وبيانات بصورة غير شرعية وهي مخزونة في دائرة الحاسوب او نسخ برامج معلوماتية بصورة غير قانونية ويتم ذلك بالحصول على كلمة السر او بواسطة التقاط موجات الكهرومغناطيسية بحاسبة خاصة . والهدف من ذلك هو سرقة الاسرار والمعلومات التجارية او التسويقية او التعرف على حسابات المنظمات والتلاعب بقيود المصارف والمؤسسات المالية او الكشف عن اسرار صناعية لتصاميم المنتجات واعادة تصنيفها دون اجازة قانونية (السالمي ، ٢٠٠٠ : ٣٩٩)

(ثالثاً) / جرائم الفضاء الرقمي : تتزايد مخاطر التقنيات الحديثة على حماية الخصوصية ، كتقنيات رقابة (كاميرات الفديو) وبطاقات الهوية الالكترونية ، قواعد البيانات الشخصية ، ووسائل اعتراض ورقابة البريد والاتصالات ، اذ يمكن استرجاع كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الخاصة والحكومية ، ونقل المعلومات المؤتمتة في قاعدة البيانات عبر البلد في ثوان وبتكاليف منخفضة نسبياً اذ ان ذلك يكشف الى اي مدى يمكن ان يكون التهديد للفضاء الرقمي (Alter , 1999 : 469).

د- مشاكل جودة النظام : فضلاً عن الكوارث والفيروسات والخروقات الأمنية لانظمة المعلومات هناك ايضاً تخلف البرامجيات والبيانات الناقصة والتي تسبب تهديدا" دائما" لنظم المعلومات مسببة خسائر لا مثيل لها في الانتاجية والخطأ غير المكتشف في برامجيات ائتمان المنظمة او البيانات المالية الخاطئة يمكن ان ينتج عنه خسائر بملايين الدولارات ، فضلا" عن العطلات والاخطاء في البرامجيات وضعف البيانات كمدخلات (Laudon & Laudon , 2005 : 530) .

ويمكن القول ان ما تتعرض له أنظمة المعلومات من مخاطر تكون متعددة فقد تكون من قبل اشخاص من خارج المنظمة يقومون باختراق نظام الحاسوب من خلال الشبكات او من قبل اشخاص داخل المنظمة يملكون صلاحيات الدخول الى النظام ولكنهم يقومون بأساءة استخدام النظام لدوافع مختلفة ، او تتعرض للمخاطر بسبب الظروف البيئية ودرجات الحرارة والرطوبة

العالية او من خلال التعرض لجرائم الحاسوب والفايروسات المضرة فضلاً عن الاختراق عبر القرصنة من خلال ما يسمى بالـ (Hackers) .

٣- حماية نظم المعلومات من الاخطار

تعتبر عملية الحماية من الاخطار التي تهدد أإمن أنظمة المعلومات من المهام المعقدة والصعبة والتي تتطلب من الادارة الكثير من الوقت والجهد والموارد المالية وذلك لعدة اسباب منها : (Labuschagne & Eloff , 2009 :157)

أ- العدد الكبير من الاخطار التي تهدد عمل نظم المعلومات

ب- التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها .

ج - التاخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمنظمة امكانية التعلم من التجربة والخبرة المتاحة .

د- تكاليف الحماية يمكن ان تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها .

هـ- صعوبة الحماية من الاخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية هذا وتقع مسؤولية وضع خطة الحماية للانشطة الرئيسة على مدير نظم المعلومات في المنظمة على ان تتضمن هذه الخطة ادخال وسائل الرقابة التي تضمن تحقيق الوقاية من الاخطار غير المتعمدة ، واكتشاف المشاكل بشكل مبكر قدر الامكان فضلاً عن المساعدة في تصحيح الاعمال واسترجاع النظام .

ويرى (Alter , 1999 : 475) انه اذا ارادت المنظمة تطوير وتاسيس نظام امن لانظمة المعلومات والحفاظ عليه فيكون من خلال الاتي : -

أ- بناء النظام بشكل صحيح وتدريب المستخدمين على القضايا الامنية .

ب- المحافظة على الامن المادي حين يكون النظام عاملا" .

ج- تجنب الدخول غير المفوض الى اجهزة الحاسوب والشبكات والبيانات بمراعاة ان النظام مؤمن مادياً .

د- الدخول المسيطر عليه والحث على تادية العمليات بكفاءة وفاعلية والسعي لتحسينها.

هـ- التدقيق الشامل والمستمر للنظام وان كان مؤمناً بالكامل لغرض ابعاد اي تدمير اوتخريب ممكن ان يحصل.

نستطيع القول انه لابد من تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات مع تركيزه على مفهوم الوقاية من الاخطار التي تتعرض لها الانظمة اذ يمكن تصميمه لحماية جميع مكونات النظام بما فيها التجهيزات والبرمجيات والشبكات .كما على المنظمة ان تحتفظ بتسهيلات دعم الطوارئ التي تحتفظ بمركز حاسبات اخر يكون كدعم في حالات الطوارئ .

٤- العناصر الاساسية لامن نظام المعلومات

يتمثل النظام الأمني الفاعل لانظمة المعلومات كونه يضم جمبع العناصر ذات الصلة بنظام المعلومات المحوسبة اذ يمكن تحديد هذه العناصر بالاتي :- Labuschagne & Eloff , (2009 :156) ، (Laudon & Laudon , 2005: 530) (Doomun , 2009 : 853) اذ اشار(Laudan & Laudan, 2005: 530) كونها تشتمل **منظومة الا جهزة الالكترونية وملحقاتها** : اجهزة حواسيب تتطور بشكل هائل بالمقابل هناك تطور في مجال السبل المستخدمة لاختراقها مما يتطلب تطوير مهارات وقابليات العاملين في اقسام انظمة المعلومات كي يستطيعوا مواجهة حالات العبث المقصود او غير المقصود في الاجهزة .

واضاف كل من (Laudon & Laudon, 2005: 530) ، (Labuschagne & Eloff , 2009 :156) كونها تمثل المستفيدين والمستخدمين لأنظمة المعلومات ، فالفرد له أاثر فاعل في اداء عمل الحواسيب وبشكل سلبي او ايجابي اذ يستطيع حماية وتوفير الأمن

لانظمة المعلومات وفي الوقت ذاته قد يكون مصدرا" للعبث لذا على ادارة المنظمة ان تضع الخطط لزيادة الحس الامني والحصانة من التخريب من خلال مراجعة وتدقيق سلوك العاملين لديها .

الا ان (Doomun , 2009 : 851 - 853) يعد البرمجيات المستخدمة في تشغيل النظام : من المكونات غير المادية والعنصر الاساس في نجاح استخدام النظام ، لذلك من الافضل اختيار حواسيب ذات انظمة تشغيل لها خصائص أمنية ويمكن ان تحقق حماية للبرامج وطرق حفظ كلمات السر وطريقة ادارة نظام التشغيل وأنظمة الاتصالات وأكد ان شبكة تناقل المعلومات ضرورة حتمية لوضع اجراءات حماية وضمان أمن الشبكات من خلال اجراء الفحوصات المستمرة لهذه المنظومات وتوفير الاجهزة الخاصة بالفحص ، كما ان نظم التشغيل المستخدمة والمسؤولة عن ادارة الحواسيب يجب أن تتمتع بكفاءة وقدرة عالية على الكشف عن التسلل الى الشبكة وذلك من خلال تصميم نظم محمية باقفال معقد أو عن طريق المجفرات وربطها بخطوط الاتصال والتي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة ومعدات لغرض تجفير تناقل المعلومات او الملفات ، فضلا" عن مواقع منظومة الاجهزة الالكترونية وملحقاتها : اذ يجب ان تتخذ الاجراءات الاحترازية لحماية الموقع وتحصينه من اي تخريب او سطو وحمايته من الحريق والتحقق من هوية الافراد الداخلين والخارجين من الموقع .

يتضح مما سبق ان العناصر الاساسية لأمن نظاام المعلومات تتمثل بـ (منظومة الاجهزة اللاكترونية وملحقاتها، والمستفيدين والمستخدمين لانظمة المعلومات ، البرمجيات المستخدمة في تشغيل النظام ، فضلاً عن تناقل شبكة المعلومالت) فالعناضر الاساسية لاي نظام تتمثل بالعاملين.

مما سبق يتبلور لنا ان العناصر الاساسية لأي نظام لأمن أنظمة المعلومات يتمثل في العاملين والمستخدمين لهذه الانظمة ومدى قدرة المنظمة من التدقيق لسلوكياتهم والمراجعة الدورية لحماية الاجهزة من التخريب المتعمد او غير المتعمد ، كما ان أمن البرمجيات أمر لابد من اخذه في الاعتبارعند تصميم النظام وكتابة برامجه من خلال وضع عدد من الاجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها وتمنع اي شخص من امكانية التلاعب والدخول الى النظام ومحاولة التمييز بين الذين يحق لهم الاطلاع وحسب كلمات السر الموضوعة وذلك عن طريق البرمجيات او استخدام الاجهزة المشفرة واجهزة الحماية والجدار الناري . اما عن شبكة تناقل المعلومات فانها تعد ثمرة التطور في مجال الاتصالات لكن بالمقابل اتاحت تسهيل عملية سرقة المعلومات وتدميرها لذا يتوجب توفير الاجهزة الخاصة بالفحص والحماية من التسلل من خلال تجفير تناقل الملفات والحفاظ على المواقع وتحصينها امنياً للسيطرة على اي تخريب او سطو قد تتعرض له .

ثانياً / الاطار العام لنظام تسجيل المخاطر معايير وقياس أمن انظمة المعلومات

سيتم بهذه الفقرة عرض المعايير والمؤشرات لأمن انظمة المعلومات والتي تمثل ثلاث طرائق اساسية لقياس الخطر والتنبيه له إذ اتفق الباحثين على الربط ما بين تلك الطرائق وكالاتي :

١- قياس أمن أنظمة المعلومات : يعد أمن نظم معلومات اي منظمة من الاهمية لذا لابد من عمل هيكل لترتيب حالات التاثير(الخطورة) وبطريقة ثابتة من خلال بعض القياسات العملية التي استخدمتها المنظمات الكبيرة في ادارة العملية الامنية لنظم معلوماتها. إذ يتطلب قياس انظمة المعلومات تحديد الحاجة الملحة والاستجابة للمخاطر الامنية فقد ركزت استراتيجيات التقييم لأمن نظم المعلومات على فحص نتائج التقييمات الامنية كـ (ممارسات الفريق الروتينية ، اختبار التوغل ، رصد قابلية التاثيراو الخطورة، الدفاع عن مواطن الضعف في الأمن ، تقييم جودة البنى التحتية) واستعراض عمليات تطوير وادارة النظام لافضل الممارسات (Hong &

245 : 2009 , other). كما ان المنظمات تحتاج الى النماذج التي تقلل من شدة الخطورة فالقياس الامني المعياري لانظمة المعلومات يمكن الحصول عليه في مختلف المستويات من خلال التفاصيل الامنية (المعيارية) للمنظمة المجمعة في النظام ، إذ ان هذه القياسات لابد ان تتصف بكونها موجهة نحو الهدف ، محددة ، يمكن قياسها ومقارنتها ، ومن ثم تحقيقها واعادتها وتعتمد على الوقت (١١ : 1994 , Meyer) إذ في السنوات الاخيرة اخذ الاهتمام باستخدام مقياس اداء أمن أنظمة المعلومات يتزايد إذ اعتبرت (NIST - SP800-33 ، ISO17799 ، BS7799) مقاييس للمعلومات في المنظمات حيث تركز بشكل اساس على تزويد مجموعات السيطرة . (245 : 2009 , Hong & other) ، لكن مقياس النوعية وتطبيق هذه السيطرة لم تعالج بالتفصيل الاخطار الامنية بمقياس كمي ، لذا كلفت جمعية الامن الهندسي لانظمة المعلومات الدولية (ISSEA) إذ تم تكليفها بمهمة تطوير القياسات الامنية لافضل نموذج من حيث القابلية الهندسية لامن انظمة المعلومات (SSE.CMM) إذ تبنت تطوير الامن والعمليات القياسية (NIST 800 - 55) من خلال الممارسات الامنية للمنظمة والممارسات التنظيمية (١٢-١١ : 1994 , Meyer) .

وتأكيداًعلى ما سبق ان اداء أامن أنظمة المعلومات الفعال يمكن قياسه من خلال استخدام المقياس الامني بمساعدة التعليمات والقواعد والممارسات والمعايير التي يتضمنها والتي تقبل على نحو واسع في العالم من خلال جهود المنظمات والشركات التي قامت بتوحيد الجهود لتطوير المقياس المعياري لأمن أانظمة المعلومات.

2 – **الاطار العام لنظام تسجيل المخاطر (CVSS) معاملاته ومؤشراته :** بدءً تحتاج المنظمات الى النماذج التي تغطي المخاطر شديدة الخطورة واحدى هذه النماذج هو نظام تسجيل درجة المخاطر (CVSS) Common Vulnerability Scoring System الذي صمم لتزويد المستخدم بجهاز تسجيل شامل يمثل شدة وخطورة المخاطر ويمكن قياسه كمياً ونوعياً .

فالقاعدة القياسية للاطار العام لنظام التنبيه عند التعرض للمخاطر (CVSS) تحتوي نوعيات جوهرية لاي مخاطر معطاة والتي لاتتغير بمرور الزمن ولبيئات مختلفة ، إذ تشخص افضل حل وسط بين الكمال وسهولة الاستعمال والدقة .

إذ اتفق الباحثين على الربط بين ثلاث طرائق اساسية لنظام تسجيل المخاطر (cvss) وكالاتي :- (Patriciu & others , 2006 : 153) ، (Ross & others , 2005 : 312) ، (Kovacich & Halibozek ,2005 : 223)

أ- طريقة تقييم اداء المخاطر لأمن انظمة المعلومات :اذ يعد نموذج تقييم اداء المخاطر نتاج منظمة (SSE - CMM) وهو قياس دولي يخاطب القدرات نظم من قبل وزارة الدفاع الامريكية ضم ثلاث مكونات رئيسة :- (Patriciu & others , 2006 : 153)

(اولاً) / القدرات (الامكانية) (AI): يقيس التاثير على التوافروالكشف بنجاح عن المخاطر للنظام المستهدف اذ يخاطب القدرات الوظيفية (يحمي ، يكشف ، يستجيب)

(ثانياً) / مستوى المساهمة (التاثير) (IB): يسمح بتسجيل الهدف لاعطاء وزن اكبر للتاثيرات (التوافر ، السرية والسلامة) على الاخريات ، اذ يخص المتطلبات التي تدعم القيام بالمهمة .

(ثالثاً) / توزيع المخاطر(الدقيق) (TD) : تخص النشاطات المطلوب قيامها لدعم متطلبات المهمة فالتحدي في تعريف القياسات الامنية لنظم المعلومات يستند على مشكلة النظام الامني ومدى قابليته للقياس مثل (النسبة المئوية ، المعدل ، الارقام الكاملة) للمقارنة ، والنتائج اذ لابد ان تكون ذات معنى ومستندة على اهداف الاداء الامني لنظم المعلومات ، ويجب ان يكون بعيداً عن التحيز في اعطاء النتائج ويغطي جميع ابعاد الامنية من خلال الاخذ بوجهات النظر العلمية والنفسية للعاملين في المنظمة.

ب- معاملات مقاييس المخاطر الامنية :

إذ تتمثل هذه الدرجة أو نظام تسجيل درجة المخاطر(CVSS) عبر مجموعة من المعاملات والمقاييس والتي منها :-

- متجه الوصول (AV): لقياس المخاطر سواء كانت موجهة محلياً او عن بعد.
- تعقيد الوصول (AC): تقيس التعقيدات والمخاطر عند دخول اي مهاجم الى النظام المقصود.
- المصداقية (الموثوقية) (A): يقيس ما اذا كانت هناك حالة لتوثيق المهاجم عند الهدف لكشف الخطورة.
- تاثير السرية (CI): تقيس تاثير السرية لاي انجاز للمخاطر والوصول للهدف. (لاشء ، جزئي ، كامل) .
- تاثير السلامة (II) : يقيس تاثير السلامة والكشف بنجاح عن المخاطر للنظام المستهدف.

ج-طريقة تقييم المخاطر الامنية / معاملات نظام التنبيه للمخاطر

يمثل الخبرة المتراكمة لنماذج من الكتاب وكذلك اختبارات واسعة للمخاطرالحقيقية في العالم ، تتمثل بمعاملات نظام التنبيه للمخاطر الامنية وكالاتي :-

(اولاً)/ المقاييس الوقتية : تقدم المخاطر المعتمدة على الوقت وتشمل :

* قابلية الانجاز Exploitability **(E)** : تقيس مدى تعقيد العملية لكشف المخاطر على النظام المستهدف .
* مستوى المعالجة Remediation Level **(RL)** : يقيس مستوى العمل المتوافر او المعالجة .
* ثقة التقرير Report Confidence **(RC)** : تقيس درجة الثقة لسعة الخطورة ومصداقية التقرير.
* النتيجة الاساسية Base Score **(BS)** : عملية احراز دمج القيم المعيارية واحتساب قيمة النتيجة الاساسية .
* النتيجة الوقتية Temporal Score **(TS)** : يسمح لتقليل تسجيل الخطورة واعادة تقييمه لفترات معينة ووقتية.

وكما في المعادلة الاتية التي تقيس المعايير الوقتية لنظام CVSS :-

$$TS = (BS \times E \times RC \times RL)$$

ويعمل هذا المقياس على التقليل من تسجيل الخطورة وهو مصمم لاعادة تقييمه لفترات معينة فالخطورة الوقتية تمثل خطورة معينة لنقاط معينة في وقت معين.

(ثانيا") /المقاييس البيئية : - تمثل المخاطر المعتمدة على البيئة وتشمل :

* توزيع الهدف (المخاطر) (Target Distribution (TD: يقيس الحجم النسبي لحقل انظمة الهدف المعرض للخطورة .
* الاضرار المحتملة (Collateral Damage Potential (CDP : يقيس احتمالية خسارة الاجهزة واضرار الملكية لنظام (CVSS)

وكما في المعادلة الاتية:-

$$ES = (TS + ((10 - TS)) \times CDP) \times TD)$$

حيث ان : النتيجة البيئية ES = Environmental Score

فالمقاييس البيئية تحسب من خلال اختبار المستخدم النهائي والاساسي وفق الصيغة اعلاه .

إذ ان النتيجة النهائية للمقياس المعياري الامني تمثل الافضلية كونه يأخذ في الاعتبار الوقت والبيئة كاستجابات اولوية ، كما انه اكثر دقة ومرونة واستجابة للمخاطر العصرية من انظمة التسجيل الاخرى .

يتضح مما سبق ان التعرض للخطر من قبل المهاجمين والضعف في المنظمات بسبب الممارسات الخطرة لغير المخولين وكذلك ما اظهرته الممارسات التي قد تحصل من قبل القراصنة جعلت اي وسيلة حماية ممكن ان تفشل لذا فالاستراتيجية الامنية ذات التوقيت الصحيح للمراقبة وجهاز المعايير الامنية سيساعد في تحديد حالة اداء الامن لنظم المعلومات ويزيد من كفاءته وذلك بتقليل منافذ التعرض لمخاطر جديدة .

إذ ان معاييرالمقاييس الامنية الممكنة تراقب تاثير الاهداف الرئيسة لامن نظم المعلومات وهي تقيس تطبيق السياسة الامنية ونتائج الخدمات الامنية وتاثير الاحداث الامنية على رسالة او مهمة المنظمة . وعادة تحتوي على قياسات متعددة وخطوط اساسية ومعلومات مساعدة تجهز الاطار لترجمة القياسات الجديدة التي تكون موجهة نحو الهدف اذ لابد ان تكون محددة ويمكن قياسها ومقارنتها كما ويمكن تحقيقها واعادتها كونها تعتمد على الوقت والنوعية .

ثالثاً / رقابة أمن انظمة المعلومات

من اجل تقليل الاخطاء والكوارث ، وسوء الخدمات ، جرائم الحاسوب والخروقات الامنية لابد من ادخال سياسات واجراءات خاصة في تصميم وتطبيق نظم المعلومات والمتمثلة بالرقابة ، فاهمية الرقابة لاتتجلى فقط في تاثيرها المباشر على كفاءة وفعالية اداء وعمل النظام بل وايضاً في حماية امن وسلامة النظام بمكوناته وموارده من البيانات والمعلومات والملفات التي تحتويها والبرامج التي تقوم بتخزينها وادارتها وتشغيلها .

١-مفهوم رقابة أمن انظمة المعلومات :سيتم بهذه الفقرة عرض مفهوم وانواع رقابة انظمة المعلومات:

يقصد **بالرقابة على انظمة المعلومات** : انها عملية المزج بين المقاييس اليدوية والمؤتمتة والتي تحمي انظمة المعلومات وتضمن عملها طبقاً للمعايير الادارية ، وتتالف من جميع الطرائق والسياسات والاجراءات التنظيمية التي تضمن سلامة موجودات المنظمة ، ودقة ومعولية سجلاتها المحاسبية ، والتكاليف التشغيلية مقارنة بالمعايير الادارية (Laudon & Laudon ,2005 :531).

ويشير (ياسين ، ٢٠٠٠ : ٣٤٥) ان الرقابة على انظمة المعلومات عموماً هي تلك العملية الادارية المستمرة والشاملة التي تستهدف السيطرة على الانشطة والعمليات المخططة والجارية في ضوء معايير محددة للانجاز.

اما الرقابة على عملية التخطيط الاستراتيجي لنظم المعلومات فيقصد بها الرقابة الاستراتيجية بقاعدة النقاط الاستراتيجية والتي تشير الى ضرورة وجود نقاط محددة يتم التركيز عليها لحساسيتها واهميتها في منع تضخيم الخطأ الحاصل او مضاعفة الانحراف المتحقق اذ تساعد هذه النقاط في الابقاء على درجة مناسبة من الرقابة الضرورية (الطائي ، ٢٠٠٠ :٢٩٣) .

ويرى (ياسين ، ٢٠٠٠ ، ٣٤٦) الرقابة الاستراتيجية على نظم المعلومات بانها تعني عمليات السيطرة التنظيمية على انشطة التخطيط الاستراتيجي للنظم بصورة كفوءة وفاعلة وبما يضمن تحقيق الاهداف الاستراتيجية ومن دون هدر في الموارد والقدرات المادية والتنظيمية ، وتطبيق نظم المعلومات وتهياة القاعدة الموضوعية للرقابة عى مراحل دورة حياة النظم وسد الفجوة بين مرحلة التخطيط لنظم المعلومات ومرحلة التطبيق بكل انشطتها الرئيسة .

يتضح مما سبق ان تخطيط وتصميم وتطبيق نظم المعلومات تتضمن الرقابة بكل انشطتها فضلاً عن العمليات التمويلية والتصميمية وتحديد اوقات البدء والانتهاء في وضع الخطط الاستراتيجية لنظم المعلومات وايجاد معايير الحماية والرقابة لانظمة المعلومات.

٢- انواع رقابة انظمة المعلومات: تجري رقابة امن نظم الحاسوب بواسطة مزيج من الرقابات العامة والتطبيقية وكالاتي:-

أ -الرقابة العامة : تحكم تصميمات وامن واستخدام برامج الحاسوب وامن ملفات البيانات عموما عبر مراحل البنى التحتية التكنولوجية لمعلومات المنظمة (Laudon & Laudon, 2005: 532) وتنصب على الجوانب الادارية وخاصة الموارد المتاحة (التنظيمية ، الافراد ، التجهيزات وغيرها من الموارد المتاحة) وضمان ان هذه الموارد يتم الحصول عليها بشكل كفوء وفاعل في بلوغ اهداف نظام المعلومات وتتضمن الاتي : (الطائي ، ٢٠٠٠ : ٢٩٦)

(اولاً) / لرقابة على نظام المعلومات.

(ثانياً) / الرقابة على مركز الحاسبة اللاكترونية .

(ثالثاً) الرقابة على امن وسلامة النظام .

ب- الرقابة التطبيقية : تعني حزمة الانشطة الخاصة بالسيطرة والحماية على نظم المعلومات في مستويات أمن وموثوقية الحواسيب وبرمجياتها فضلاً عن امن الملفات والبيانات والمعلومات والتأكد من كفاءة عمليات الحواسيب (ياسين ، ٢٠٠٠ :٣٤٩)

ويشير (Laudon & Laudon , 2005 :534)على انها مجموعة الاجراءات المؤتمتة واليدوية التي تضمن ان البيانات تجري معالجتها بصورة كاملة ودقيقة من خلال التطبيق وتصنف الى :-

(اولاً)/ رقابة المدخلات : اي التاكد من دقة واكتمال البيانات اثناء المعالجة والتشكيل والتحديث (ياسين ، ٢٠٠٠ :٣٥٠) .

(ثانتياً) / رقابة المعالجة : تكون بيانات دقيقة ومكتملة اثناء التحديث واجمالي الرقابة والتطبيق ، وتوليف الحاسوب ، فحص البرمجيات والتاكد من استعمالها للغرض المخطط لها .

(ثالثاً) / رقابة المخرجات : نتائج معالجة الحاسوب يجب ان تكون دقيقة وكاملة موزعة بصورة مناسبة اذ تتمثل باجراءات عدة كاستخدام الشاشة المرئية لاكتشاف وتصحيح الاخطاء والتحكم في توزيع المعلومات (المخرجات) الى الجهات المستقيدة لاجل ضمان ان الجهة المستلمة هي جهة مرخصة باستخدامها ، ومقارنة جميع المخرجات مع مجاميع المدخلات لايجاد التوافق بينهما والتاكد من عدم فقدان اي بيانات اثناء المعالجة والانتقال بين المراحل (Laudon & Laudon , 2005 :534).

نلاحظ مما سبق ان الرقابة العامة على انظمة المعلومات يجري تصميمها وادامتها من قبل اخصائيي نظم المعلومات اذ ان الرقابة والأمن على نظم المعلومات تتطلب وجهات نظر المستخدمين النهائيين ومدراء النشاط، في حين الرقابة التطبيقية تتضمن أمن تسجيل ومعالجة البيانات واعداد التقارير وتوصيلها وتخزين المعلومات بما يتناسب والحاجة اليها والهدف الاساس من الرقابة على المدخلات هو منع حدوث الاخطاء عند ادخال البيانات والتي قد تنسحب على عمليات المعالجة اللاحقة فمن خلال استخدام الرقابة على تشغيل البرامج يمكن استخدام الحاسبة ايضا" للمساعدة في كشف اخطاء المدخلات وبنفس الوقت كشف الاخطاء التي قد تحصل عند معالجة هذه المدخلات .

المبحث الثالث/الجانب العملي

اولاً / نبذة عن مصرف الرافدين / فرع شارع فلسطين

تاسس مصرف الرافدين الرئيسي عام (١٩٤١) في العراق وفيه فروع متعددة يقوم المصرف باعمال متعددة منها السفاتج ، حوالات ، السلف ، الحسابات الجارية ، والتوفير والائتمان ، فضلا" عن اتباع البطاقة الذكية في صرف رواتب المتقاعدين وبالتعاون مع شركة (كي) الخاصة والحسابات والقروض . ويقوم المصرف باستخدام الجدران النارية وكلمات السر كطرق حماية لامنية المعلومات وسريتها وان استخدامهما مقصور على اشخاص معينين في المصرف وعندما يراد سحب مبلغ يتجاوز ٢٥٠ مليون دينار لا يتم ذلك الا من قبل

المدير العام واستخدامه لكلمة السر وهو المسؤول عن صرف هكذا مبالغ واذا ازدادت المبالغ التي يراد سحبها فيجب ان تكون هناك موافقة من المدير العام للمصرف الرئيسي .

ثانياً/ تحليل وتقييم مؤشرات المتغيرات الاساسية للبحث

لغرض تقييم امنية انظمة المعلومات في مصرف الرافدين ولغرض تطبيق نظام التسجيل الامني المعياري (CVSS) تم الاعتماد على استخدام قوائم الفحص (Checklist) والمتضمنة الفقرات المكونة للنظام والموضحة في الملحق (١) والتي تعد وسيلة للتعرف على الواقع الفعلي لانظمة المعلومات المتبعة في المصرف والتي من خلالها يتم تطبيق المعادلة الكمية لنظام المقياس المعياري والتي تم تناولها في فقرة منهجية البحث .

اذ تم تحليل النتائج باستخدام المتوسط الموزون وكالاتي :-

$$X\ bar = \sum(x\ i \times w\ i) \ / \sum (w\ i)$$

حيث ان : w i = التكرارات لكل فئة ، xi = الوزن لكل فئة ،وروعي ان تتضمن المعاملات لمقاييس الخطورة ومعايير مقاييس تقييم اداء الخطورة فضلاً عن الاستراتيجيات المتبعة لامن انظمة المعلومات ، اذ تم صياغة اسئلة استمارة الفحص وفق المؤشرات والمعاملات المذكورة في منهجية البحث وتم تحديد ثلاث اوزان لغرض قياس المتوسط الموزون وعلى النحو المبين ادناه :-

أ- <u>تحليل معاملات مقاييس الخطورة</u>

تضمنت هذه الفقرة مجموعة من الاسئلة التي يتم من خلالها تقييم مقاييس الخطورة المتبعة في المصرف وكما موضح في الجدول رقم (١) جاءت نتائج الاجابات عن السؤال (١) ضمن هذه المجموعة والذي استهدف الكشف عن مدى سهولة استخدام الاجراءات الامنية اذ تميل معظمها نحو الوزن الثاني (متوفر الى حد ما) (٢.٠٧) وفيما يتعلق بدقة الاجراءات الامنية المتبعة في المصرف جاءت الاجابات حول السؤال (٢) بانها متوفرة بصورة كافية (١.٦١) اما اجابات السؤال (٣) والمتعلق بطبيعة الخطر الامني وتوجيهه من الداخل كانت الاجابة محصورة بين متوفر بصورة كافية وعدم توفر ذلك الا ان اغلب الاجابات تتجه نحو توفر ذلك الى حد ما (٢.١٥)

وفيما يخص طبيعة الخطر وتوجيهه من الخارج كانت الاجابات على السؤال (٤) متوفر بصورة كافية (١.٦٩) ، وفيما يتعلق بتوفر اجراءات امنية داخل المصرف لمنع الاختراقات والدخول غير المفوض فكانت اكثر الاجابات تؤكد انها متوفرة بصورة كافية (١.٧٦) . اما عن توثيق حالات الاختراق التي تصيب نظام المعلومات فهي غير متوفرة بصورة كافية (2.92) .

اما نتيجة اجابات السؤال (٧) والمتعلق بوجود نظام للكشف عن المخاطر اكدت عدم توفر ذلك بصورة كافية (٢.٥٣) . وفيما يخص تاثير المخاطر على سرية العمل فكانت الاجابات تتجه نحو الوزن الاول متوفر بصورة كافية (١.٣٨) ، وفيما يتعلق بامكانية اي فرد من العاملين في المصرف الدخول لنظام المعلومات المستهدف جاءت الاجابة عن السؤال (٩) بعدم امكانية ذلك (٢.٣٠) .

جدول رقم (١) تحليل مؤشرات معاملات مقاييس الخطورة

الاوزان / الاسئلة		الوزن الاول		الوزن الثاني		الوزن الثالث		المتوسط الموزون
		التكرار	النسبة%	التكرار	النسبة%	التكرار	النسبة%	
AV	١	٢	١٥.٣	٨	٦١.٥	٣	٢٣.٢	٢.٠٧
	٢	٨	٦١.٥	٢	١٥.٣	٣	٢٣.٢	١.٦١

	٣	٦	٤٦.١٥	-	-	٧	٥٣.٨٥	٢.١٥
	٤	٨	٦١.٥	١	٧.٦٥	٤	٣٨.٤٦	١.٦٩
AC	٥	٦	٤١.١٥	٤	٣٠.٨٥	٣	٢٣.٧	١.٧٦
A	٦	-	-	١	٧.٦٥	١٢	٩٢.٣٠	٢.٩٢
	٧	-	-	٦	٤٦.١٥	٧	٥٣.٨٤	٢.٥٣
CI	٨	٨	٦١.٥	٥	٣٨.٤٦	-	-	١.٣٨
	٩	٢	١٥.٣	٢	١٥.٣	٩	٦٩.٢٣	٢.٥
II	١٠	٢	١٥.٣	٥	٣٨.٤٦	٦	٤٦.١٥	٢.٣٠
	١١	-	-	٩	٦٩.٢٣	٤	٣٠.٨٥	٢.٣٠

المصدر : من اعداد الباحثة

* يشير الوزن الاول (١) الى (متوفر بصورة كافية) ، الوزن الثاني (٢) الى (متوفر الى حد ما) ، الوزن الثالث (٣) الى (غير متوفر بصورة كافية) .

اذ تم استخراج الارقام وفق المعادلة اعلاه وكما في المثال :

(٢ × ١) + (٨ × ٢) + (٣ × ٣) = ٢.٠٧ وهكذا استخرجت بقية الارقام

ولغرض التعرف على القدرة في تشخيص المخاطر التي تصيب النظام المستهدف وبنجاح داخل المصرف كانت الاجابة على السؤال (١٠) اغلبها تؤكد بعدم توفر ذلك بصورة كافية (٢.٣٠) وعن امكانية توافر وكشف المحاولات الناجحة داخل المصرف لمخاطر التاثير بالنظام المستهدف جاءت الاجابة عن السؤال (١١) تؤكد اغلبها توفر ذلك الى حد ما (٢.٣٠) .

٢- تحليل معايير مقاييس تقييم اداء المخاطر

تضمنت هذه المعايير مجموعة من المقاييس لتقييم اداء الخطورة كما مبين في الجدول رقم (٢) وعلى النحو الاتي :-

أ – **القدرات :** يخص السؤال (١٢) مدى استخدام المصرف لبرنامج حماية لامن نظام المعلومات فكانت الاجابات معظمها نحو الوزن الاول (١.٨٤) ، اما السؤال (١٣) الذي يتعلق بمدى الاستجابة والقدرة للتصدي لاي قرصنة فنلاحظ ان الاجابات تتجه نحو الوزن الاول متوفر بصورة كافية (١.٩٢) .

اما الاجابات التي تخص السؤال (١٤) والمتعلق بمدى امكانية المصرف لمكافحة الخروقات الامنية فنلاحظ انها تتمركز نحو الوزن الاول متوفر بصورة كافية (١.٦٩) ، ولغرض التعرف على مدى وجود قسم مختص بامنية المعلومات كانت اجابات العينة للسؤال (١٥) هي غير متوفر بصورة كافية (٢.٤٦) ، اما بخصوص قدرة المصرف على كشف الخروقات الامنية فنلاحظ الاجابات الخاصة بالسؤال (١٦) تتجه نحو الوزن الثالث غير متوفر (٢.٤٦) .

جدول رقم (٢) تحليل المؤشرات المتعلقة بقدرا ت النظام

الاوزان / الاسئلة		الوزن الاول		الوزن الثاني		الوزن الثالث		المتوسط الموزون
		تكرار	النسبة%	تكرار	النسبة%	تكرار	النسبة%	
AI	١٢	٦	٤٦.١٥	٣	٢٣.٠٧	٤	٣٠.٧	١.٨٤
	١٣	٦	٤٦.١٥	٢	١٥.٣	٥	٣٨.٤٦	١.٩٢
	١٤	٦	٤٦.١٥	٥	٣٨.٤٦	٢	١٥.٣	١.٦٩
	١٥	٣	٢٣.٦٧	١	٧.٦٩	٩	٦٩.٢٣	٢.٤٦
	١٦	٢	١٥.٣	٣	٢٣.٠٧	٨	٦١.٥	٢.٤٦

المصدر : من اعداد الباحثة

ب - مستوى المساهمة : تضمنت مجموعة من الاسئلة الموضحة في الجدول رقم (٣) وعلى النحو الاتي :-

كانت الاجابات المتعلقة بالسؤال (١٧) حول مدى توفر متطلبات تسهل الحماية لامنية نظم المعلومات تتركز حول الوزن الاول متوفر بصورة كافية (٢.٣٠) . وعن مدى استخدام المصرف برامج الجدار الناري لتوفير الحماية كانت الاجابة الخاصة بالسؤال (١٨) هي غير متوفربصورة كافية (٢.٩٦) .

ويلاحظ من نتائج الاجابات بمدى استخدام كلمة السر للحماية في المصرف للسؤال (١٩) انها متوفرة بصورة كافية (١.٣٠) . وللتعرف على مدى استخدام برامج مكافحة الفايروسات التي يتعرض لها النظام كانت الاجابة للسؤال (٢٠) تتراوح بين متوفر بصورة كافية وغير متوفر (٢) . ولغرض القيام بتقييم القياسات الامنية لانظمة المعلومات يجري تطوير افضل الممارسات للحد من عمليات القرصنة والسطو كانت الاجابات للسؤال (٢١) متوفرة بصورة كافية (٢) .

جدول رقم (٣) تحليل المؤشرات المتعلقة بمستوى مساهمة النظام

الاوزان / الاسئلة		الوزن الاول		الوزن الثاني		الوزن الثالث		المتوسط الموزون
		التكرار	النسبة %	تكرار	النسبة%	تكرار	النسبة%	
IB	١٧	٤	٣٠.٧	١	٧.٦٩	8	٦١.٥	2.30
	١٨	-	-	٤	٣٠.٧	9	٦٩.٢٣	2.69
	١٩	٩	٦٩.٢٣	١	٧.٦٩	3	٢٣.٠٧	1.53
	٢٠	٦	٤٦.١٥	١	٧.٦٩	6	٤٦.١٥	٢
	٢١	٦	٤٦.١٥	٤	٣٠.٧	4	٣٠.٧	2

المصدر : من اعداد الباحثة

ج- نظام توزيع المخاطر الدقيق :شملت هذه المؤشرات مجموعة من الاسئلة التي تتعلق بنظام المخاطر الدقيقة في مصرف الرافدين وعلى النحو المبين في الجدول (٤) وكالاتي :-وضع السؤال (٢٢) للتعرف على مدى قياس النظام الامني المستخدم بنسبة مئوية فجاءت الاجوبة معظمها متجهة نحو الوزن الثالث (غير متوفر بصورة كافية) (٢.٣٠) . اما عن نتائج الاجابات عن السؤال (٢٣) والمتعلقة بمدى توفر الحماية والسرية في نتائج القياس المستندة الى اهداف الاداء الامني فكانت تميل معظمها الى الوزن الثالث (غير متوفر بصورة كافية) (٢.٢٣)

جدول رقم (٤) تحليل مؤشرات نظام المخاطر الدقيقة باستخدام المتوسط الموزون

الاوزان / الاسئلة		الوزن الاول		الوزن الثاني		الوزن الثالث		المتوسط الموزون
		تكرار	النسبة	تكرار	النسبة	تكرار	النسبة	
TD	٢٢	2	١٥.٣	5	٣٨.٤٦	٦	٤٦.١٥	2.30
	٢٣	3	٢٣.٧	4	٣٠.٧	٦	٤٦.١٥	2.23

المصدر : من اعداد الباحثة

٣- تحليل مؤشرات الخطورة ضمن مقياس نظام المخاطر الامنية لانظمة المعلومات:

أ- نظام المخاطر الوقتية : تضمنت مجموعة من الاسئلة تعلق السؤال رقم (٢٤) بمدى القيام بكشف المخاطر على نظام المعلومات المستهدف في مصرف الرافدين وكانت اجابات العينة تتجه نحو الوزن الثالث (غير متوفر بصورة كافية) (٢.٣٠) ، اما السؤال رقم (٢٥) الذي يهدف الى التعرف على مدى توفيرتخصيص موارد كافية لمواجهة المخاطر الامنية لنظام المعلومات فكانت الاجابة تتمركز نحو الوزن الثالث غير متوفر بصورة كافية (٢.٦٩). اما فيما يخص السؤال (٢٦) والمتعلق بمدى المصداقية في التقارير المستخرجة من القياسات الامنية فتركز في الاجابات نحو الوزن الثاني والوزن الثالث بمقدار (٢.١٥) .
بينما اتجهت الاجابات المتعلقة بالسؤال رقم (٢٧) الخاص بمدى امتلاك المصرف للنماذج التي تستطيع الاعتماد عليها في قياس شدة الخطورة واختراق النظام في المصرف فاتجهت نحو الوزن الثاني متوفر الى حد ما (٢.٢٣) ، فيما تعلق السؤال رقم (٢٨) بامتلاك المصرف متخصصين لمواجهة المخاطر الامنية التي يتعرض لها نظام المعلومات فاتجهت نحو الوزن الاول (متوفر بصورة كافية) (١.٥٣) ، ولغرض التعرف على مدى اقبال المصرف في سياساته لحماية امن البرامج والمعلومات من وجود فريق يقوم بتحمل هذه المسؤولية من خلال السؤال رقم (٢٩) جاءت معظم الاجابات نحو الوزن الاول متوفر (١.٣٨) ، وكما موضح في الجدول رقم (٥) .

جدول رقم (٥) تحليل مؤشرات نظام المخاطر الوقتية

الاوزان / الاسئلة		الوزن الاول		الوزن الثاني		الوزن الثالث		المتوسط الموزون
		تكرار	النسبة	تكرار	النسبة	تكرار	النسبة	
E	24	2	١٥.٣	5	٣٨.٤٦	6	٤٦.١٥	2.30
	٢٥	١	٧.٦٩	٤	٣٠.٧	٩	٦٩.٢٣	٢.٦٩
RC	٢٦	3	٢٣.٧	٥	٣٨.٤٦	٥	٣٨.٤٦	٢.١٥
RC	27	١	٧.٠	٨	٦١.٥	٤	٣٠.٧	٢.٢٣
RL	٢٨	٩	٦٩.٢٣	١	٧.٦٩	٣	٢٣.٠٧	١.٥٣
	٢٩	١٠	٧٦.٩٢	١	٧.٦٩	٢	١٥.٣	١.٣٨

المصدر : من اعداد الباحثة

ب- **المخاطر البيئية :**تضمنت تحليل مجموعة من المؤشرات المتعلقة بمواجهة المصرف للمخاطر البيئية وكما هو في الجدول رقم (٦) وعلى النحو الاتي :-
تعلق السؤال رقم (٣٠) بمدى امكانية المصرف من صيانة انظمة معلوماته فكانت الاجابات معظمها تتجه نحو الوزن الثاني (متوفر الى حد ما) (٢.٣٠) ، اما فيما يخص السؤال رقم (٣١) حول احتمالية فقدان وخسارة الاجهزة والمعلومات فنلاحظ ان معظم الاجابات تركزت نحو الوزن الثالث غير متوفربصورة كافية (٢.٥٣).

جدول رقم (٦) تحليل مؤشرات نظام المخاطر البيئية

الاوزان / الاسئلة		الوزن الاول		الوزن الثاني		الوزن الثالث		المتوسط الموزون
		تكرار	النسبة	تكرار	النسبة	تكرار	النسبة	
CDP	٢٦	١	٧.٦٩	٧	٥٣.٨٤	٥	٣٨.٤٦	2.30
	٢٨	١	٧.٦٩	٤	٣٠.٧	٨	٦١.٥	٢.٥٣

المصدر : من اعداد الباحثة

وبعدان تم اعطاء اوزان للمعايير المستخدمة في المقياس CVSS سيتم تحليل واقع حال نظام المعلومات الامنية وتقييمه بنفس الوقت من خلال استمارة الفحص (Checklist) والتي تمثل مقياس النظام المعياري لحماية وامنية نظام المعلومات في المصرف المبحوث والذي تم الاعتماد فيه على مقياس عالمي هو (CVSS) (Common Vulnerability Scoring System) نظام التنبيه عند التعرض للمخاطر من خلال تطبيق المعادلات الاتية :- **BS = (10 + AV × AC×A) × ((CI× (CI IB) + (II) + (II IB) + (AV + AI IB)**

اذ سيتم قياس المؤشر واحتسابه من خلال النسبة لكل سؤال وفق المؤشرله وكالاتي :

$$AV = 1.69 + 2.15 + 1.61 + 2.07 / 4 = 1.88$$

$$AC = 1.76$$

$$A = 2.53 + 2.92 / 2 = 2.36$$

$$CI = 2.5 + 1.38 / 2 = 1.94$$

$$II = 2.30 + 2.30 / 2 = 2.3$$

$$AI = 2.46 + 2.46 + 1.69 + 1.92 + 1.84 / 5 = 2.07$$

$$IB = 2 + 2 + 1.55 + 2.69 + 2.30 / 4 = 2.10$$

$$TD = 2.23 + 2.30 / 2 = 2.26$$

$$E = 2.30 + 2.69 / 2 = 2.15$$

$$RC = 2.23 + 2.15 / 2 = 2.39$$

$$CDP = 2.53 + 2.30 / 2 = 2.41$$

$$RL = 1.53 + 1.38 / 2 = 1.45$$

$$\mathbf{BS} = (10 + ((1.88 \times 1.76 \times 2.36)) \times ((1.94 \times 2.10) + (2.3) + (2.37 \times 2.10) + (1.88 + (2.07 + 2.10))$$

$$\mathbf{BS} = 85.79$$

وبعد ان تم اسنخراج النتيجة الاساسية لقياس المعايير الامنية لانظمة المعلومات وتعقيد الوصول ومدى تاثره بوجود السرية في المعلومات والمصداقية في حال التوثيق والكشف عن المخاطر سوف نستخرج قيمة TSمن المعادلة الاتية :

$$TS = (BS \times RC \times RL)$$

$$= (85.79 \times 1.53 \times 2.39)$$

$$= 313.7$$

وتمثل نتيجة الوقت اذ تعمل على تقليل تسجيل الخطورة لنقاط معينة في وقت معين . اما المقاييس البيئية والتي تقيس الحجم النسبي لحقل انظمة الهدف المعرض للخطورة فتقيس احتمالية خسارة الاجهزة واضرار ملكية نظام CVSS اذ يمكن التعرف عليها من خلال تطبيق المعادلة الاتية :-

$$ES = (TS + ((10 - TS)) \times CDP) \times TD)$$

$$= (313.7 + ((10 - 313.7)) \times 2.41) \times 2.26)$$

$$= 54.46$$

اذ تصبح نتيجة المعايير البيئية الذي تم احتسابها من خلال اختبار المستخدم النهائي والاساسي وفق الصيغة اعلاه. وان النتيجة النهائية لمقياس الامن المعياري يمثل الافضلية كونه ياخذ في الاعتبار المخاطر الدقيقة والوقت والبيئة كاستجابات اولوية . كما انه اكثر دقة ومرونة واستجابة للمخاطر العصرية من انظمة التسجيل الاخرى، اذ يتم مقارنة هذه النتيجة بالمقياس العالمي لمواصفات المعهد البريطاني الذي نشر عام ١٩٩٥ لامن المعلومات ما بين (١- ٧٧٧٩٩) وكما في المعادلة الاتية :- (٢٤٣ : ٢٠٠٩ ، Louss & Hsing)

$$CVSS = BS \times TS \times ES$$

$$= 85.79 \times 313.7 \times 54.46$$

$$= 14656.451$$

ويتضح من خلال المقارنة بين رقم المواصفات العالمية وبين النتيجة التي تم التوصل اليها لمقياس نظام المعلوما المطبق في المصرف عينة البحث انه لايستخدم مقياس حماية امن المعلومات بشكل فاعل وانه يستند في حماية البيانات والمعلومات على كلمات السر والوسائل البسيطة في الحماية والجدار الناري والتي لاتمكن من كشف المخاطر بدقة .

٤- تحليل العلاقات بين مؤشرات استخدام نظام التنبيه عند التعرض للمخاطر

اختباراً لفرضية البحث تشير معاملات الارتباط الواردة في الجدول (٧) فيما بين مؤشرات المقاييس الامنية لنظام التنبيه عند التعرض للمخاطر في المصرف المبحوث عن وجود ثمان علاقات معنوية من اصل ١٥ علاقة اذ سجلت العلاقة بين كل من تقييم اداء المخاطر (القدرات – المساهمة) مقداراً (٠.٧٦) وبين القدرات وتحديد المخاطر الدقيقة بلغ معامل الارتباط (٠.٦٠٣) والعلاقة بين القدرات وتقييم المخاطر الدقيقة سجلت (٠.٧١٥) ، والمساهمة والمخاطرالدقيقة (٠.٨٢) ، اما المساهمة والمخاطر البيئية فبلغ (٠.٧٦٢) وسجل معامل الارتباط بين المخاطر الدقيقة والوقتية مقدار (٠.٨٨٣) والمخاطر الدقيقة والبيئية بلغ (٠.٦٦٧)، اما المخاطر الوقتية وعلاقتها بالمخاطر البيئية سجلت ارتباط (٠.٦٥٥) وجميع هذه العلاقات موجبة وقوية ودالة معنوياً وعند مستوى معنوية (٠.٠١) مما يشير الى وجود علاقات ارتباط بين معاملات ومؤشرات مقاييس المعايير الامنية والذي يعد مؤشراً حقيقياً لتطبيق نظام التنبيه وتسجيل المخاطر .

جدول (٧) معاملات الارتباط بين مؤشرات مقياس المعايير الامنية لنظام المعلومات

المؤشرات المقياس الامني		معاملات مقاييس الخطورة	مقاييس تقييم اداء الخطورة			معاملات نظام المخاطر	
			القدرات	المساهمة	المخاطرالدقيقة	مخاطروقتية	مخاطربيئية
معاملات مقاييس الخطورة		١.٠٠٠	٠.٢٤ -	٠.٥١٢	٠.٤٧	٠.٢٩	٠.٥٦٧
مقاييس تقييم اداء الخطورة	القدرات		١.٠٠٠	** ٠.٧٥٩	** ٠.٦٠٣	** ٠.٧١٥	٠.٤٦٧
	المساهمة			١.٠٠٠	٠.٨٢ **	٠.٣٧٨ -	** ٠.٧٦٢
	المخاطر الدقيقة				١.٠٠٠	** ٠.٨٨٣	** ٠.٦٦٧
معاملات نظام التنبيه للمخاطر	المخاطر الوقتية					١.٠٠٠	** ٠.٦٥٥
	المخاطر البيئية						١.٠٠٠

المصدر : من اعداد الباحثة

اما معامل الارتباط بين قدرات تقييم اداء الخطورة ومعاملات مقياس الخطورة بلغ (٠.٢٤-) وهو ارتباط سالب ضعيف ، ولكنه دال معنوياً لان قيمة (p = 0.002) وهذه العلاقة ذات دلالة معنوية اذ ان معاملات مقاييس الخطورة ممكن ان تؤثر في تقييم القدرات على الامد البعيد ، وسجلت العلاقة بين المساهمة وتحديد المخاطر الدقيقة ايضاً ارتباط سالب بلغ (٠.٣٧٩-) وهو متوسط القوة وغير دال معنوياً اذ بلغت قيمة (p = 0.423) وهي اكبر من (٠.٠٥) ، في حين بلغ معامل الارتباط بين (معاملات مقاييس الخطورة والمساهمة) (٠.٥١) وهو معامل ارتباط موجب ودال معنوياً اذ بلغت قيمة (p = 0.001) ويدل ذلك على ان هناك ارتباط طردي فيما بين المتغيرين . وسجلت معاملات مقاييس الخطورة مع توزيع المخاطر الدقيقة ما مقداره (٠.٤٧) وهو ارتباط موجب متوسط القوة لكنه دال معنويا اذ بلغت قيمة (p = 0.003) ومن نتيجة العلاقة هذه نستطيع القول هنالك تفعيل لمعاملات

المقاييس التي تتعلق بالمخاطر مع تحديد تلك المخاطر بدقة الا ان توظيف ذلك في المصرف المبحوث لم يصل للمستوى المطلوب . وحققت العلاقة بين معاملات مقاييس الخطورة والمخاطر الوقتية معامل ارتباط بلغ (٠.٢٩) وهو ارتباط موجب ضعيف وغير دال معنوياً ، وبلغ معامل الارتباط (٠.٥٦٧) بين معاملات مقياس الخطورة والمخاطر البيئية وهو ارتباط موجب متوسط القوة ودال معنوياً مما يشير الى تاثير البيئة في مقياس الخطورة .

يلاحظ وجود علاقات فاعلة فيما بين المؤشرات والمعاملات لكن المصرف المبحوث لايقوم بتطبيق النظام وتفعيل المقياس المعياري لأمن انظمة المعلومات بالصورة وذلك يعود لعدة اسباب الى ضعف تفعيل واستخدام نظام امني خاص بانظمة معلومات المصرف المبحوث ولعدة اسباب منها الاتي :-

أ- انخفاض حماية المعلومات بسبب عدم استخدام مقياس أمني ملائم في عمل المصرف اذ لو تم التعرض للمخاطر سوف يلجأ المصرف المبحوث الى فريق عمل متخصص من خارج المصرف.

ب- ارتفاع تكاليف صيانة الاجهزة والمعدات عند التعرض للمخاطر .

ج- تتكرر العطلات في الاجهزة باستمرار لعدم توفر الحماية مما يستدعي الى تاخير انجاز الاعمال .

المبحث الرابع/الاستنتاجات والتوصيات

اولاً / الاستنتاجات :-

من خلال المعايشة الميدانية في المصرف المبحوث ومن تقييم واجابة استمارة الفحص تبين الاتي :

١- اظهرت النتائج ان نظام معلومات المصرف المبحوث لايستخدم الا من قبل المخول في قسم نظام المعلومات ، مما يؤكد ان هناك حماية للنظام الامني من الاختراق غير المفوض لكن دون الاعتماد على نظام معلومات حقيقي ومقاس بطريقة علمية.

٢- اتضح ان المصرف لا تتوافر فيه برامج الكشف عن الخروقات الامنية بشكل مبكر مما يؤكد ضرورة تعزيز المصرف لاستخدام نظام التنبيه عند التعرض للمخاطر.

٣- اظهرت النتائج صحة فرضيات البحث اذ ان أمن حماية المعلومات يساعد في الحد من المخاطر ومواجهتها.

٤- دلت الاجراءات الامنية داخل المصرف عن وجود توثيق بسيط لحالات الاختراق التي قد توجد في المصرف.

٥- ظهر ان المصرف يستعمل اجراءات الحماية البسيطة كاستعمال كلمة السر والتي من السهل اختراقها من قبل اي مبرمج متمكن .

٦- نتائج قياس اهداف الاداء الامني تؤكد الى عدم توفرها بصورة كافية في المصرف المبحوث .

٧- ظهر اانخفاض القيام بكشف المخاطر بالسرعة المطلوبة مما يستدعي قيام المصرف المبحوث بتعزيز استخدام الوسائل التي تؤدي الى توافر نظام المخاطر المتعلقة بالوقت .

٨- اسفرت النتائج عن عدم توفر صيانة كافية في المصرف لحماية انظمة المعلومات واذا ما حدث خلل او اختراق للاجهزة يستعين المصرف بفريق عمل من خارجه.

ثالثياً : التوصيات

١- العمل الجاد للاستفادة القصوى من استخدام نظام الامن المعياري وتطبيقه في المصرف لحماية انظمة معلومات المصرف كونه ياخذ في الاعتبار المخاطر الدقيقة والبيئية والوقتية ويعد من افضل انظمة الحماية المستخدمة عالمياً .
٢- العمل على خفض الخروقات الامنية من خلال تدريب العاملين في المصرف على استخدام برامج الحماية الفاعلة والكفوءة .
٣- تفعيل تقييم القياسات الامنية لانظمة المعلومات وتطويرها يعد سلاحا" للحد من عمليات القرصنة والسطو التي قد يتعرض لها المصرف .
٤- التهيؤ والعمل على تقليص العطلات التي تصيب الاجهزة والمعدات بالاعتماد على المقاييس الامنية المقترحة في البحث وتطبيقها .
٥- اعتماد نظام أمني متكامل يضم فريق متخصص للعمل وفق الاساليب التي تؤدي الى خفض تكاليف الصيانة وارتفاع امنية المعلومات والمحافظة على سريتها ويكون من داخل المصرف .
٦- تفعيل وتطبيق المؤشرات الجديدة لتحسين أمنية نظام المعلومات في المصرف لاسيما الصيغ والمقاييس الكمية التي تعكس واقع الاداء الداخلي لمسار عمل المصرف ، وامكانية استخدامها في المصارف العراقية الاخرى .
٧- تعزيز برمجة عمل الصيانة لضمان خفض العطلات والتوقفات الفجائية التي من شانها ان تعرض النظام الى فقدان المعلومات وخسارتها .
٨- توثيق حالات الاختراق التي قد تصيب نظام المعلومات في المصرف كونها غير متوفرة فيه بصورة دقيقة .
٩- تعزيز المصرف لاستخدام برامج الحائط الناري كوسيلة حماية اكثر فاعلية .
١٠- الاستمرار في دراسة حماية امن انظمة المعلومات وعلى الاخص منظومة المصارف للاستفادة من المقياس المعياري لقياس المخاطر والتنبيه عند التعرض لها .

المصادر العربية :

١- ياسين ، سعد غالب ، تحليل وتصميم نظم المعلومات ، دار الناهج ، ط١ ، ٢٠٠٠ .
٢- السالمي ، علاء عبد الرزاق ، الشبكات ونظم المعلومات ، دار الناهج ، ط١ ، ٢٠٠٠ .
٣- الطائي ، محمد حسين ، نظم المعلومات الادارية ، دار اليازوري ، ط١ ، ٢٠٠٠ .

المصادر الاجنبية

4- Alter, Steven, " Information System: A Management Perspective " 3rd.ed. Addison - Wesley Publisher , INC, New York, 1999.
5- Doomun, M. Razvi, " Multi- Level Information System Security in outsourcing domain: Business Process Management ", Journal, No1. 15 , No.1, 2009, PP.849 -857.
6- Gerold, Kovacich &Edward & Alibozek , " Security Metrics Management : How To Measure The Costs and Benefits of Security," Butterworth –Heinemann, 2005.
7- Labusshagne, L. & Eloff , J ," Electronic Commerce : The Information – Security Challenge", Information Management & Computer Security V0l.17 ,No.1, 2009, PP.154 – 157 .

8- Laudon, K.C. & Laudon , J.P., "Management Information System ",6th ed., Prentice – Hill , International , New Jersey, 2005.
9- Meyer, N .D, "A Sensible approach to out sourcing: Information System Management ", Vol.11 .No.4. 1994, pp. 7 – 22.
10- Warman, A.R, "Computer Security Within Organization ", Macmillan Press, Basing Stock, 1993.
11- Patriciu & Priesccu & Nicolaescu, "Security Metrics for Entries Information Systems", Vol, 1, No.2, 2006, PP. 43-49.
12- Ron Ross, & others, "Recommended Security Controls for Federal Information System", Nest Special Publications /2005.
Http: // esc.nist.gov/publications / disturbs / 800 -53. pdf).(
13- O'Brien, J. A," Introduction to Automation system: Essential for the internet worked enter Pries ", 11th .ed. Me Grew –Hall, Boston, 2003.
14-Swanson & Hash & Bowen, "Information Security", United States of America, National Institute of Standards and Technology", February .2006.
15-Ruth, c. Mitchell, Rita, Marcella & Graeme Baxter, "Corporate Information Security management ", New Library World, V.110 , N .1 ,2009 , PP.213 -227.
16 - Louis & Hhsing ," An integrated system theory of information security management, 2006.

ملحق (١) استمارة الفحص

الرمز	اسئلة استمارة الفحص	متوافر	متوافرالى حد ما	غير متوافر
	معاملات مقاييس الخطورة : ١- الاجراءات الامنية تتصف بالسهولة فيما يخص البيانات والمعلومات.			
	٢- حصانة الاجراءات الامنية في المصرف .			
	٣- أيوجد خطا أمني متوجه من الداخل اي العاملين.			
	٤- أيوجد خطا أمني متوجه من الخارج العملاء / القراصنة .			
	٥- توجد اجراءات امنية لمنع الاختراقات والدخول غير المفوض.			
	٦- هناك توثيق لحالات الاختراق التي تصيب نظام المعلومات .			
	٧- يوجد نظام للكشف عن المخاطر.			
	٨- تؤثر المخاطر على سرية العمل .			
	٩- يتمكن جميع العاملين في المصرف من الدخول الى نظام المعلومات للمصرف المبحوث .			
	١٠- يتم تشخيص المخاطر التي قد تصيب نظام المعلومات المستهدف بنجاح .			
	١١-مدى امكانية توافر وكشف المحاولات الناجحة لمخاطر التأثير بالنظام المستهدف .			

	معايير مقاييس تقييم أداء الخطورة: **أ- القدرات:** ١٢- يتم استخدام برنامج الحماية لأمن نظام المعلومات . ١٣- هناك قدرة للتصدي لاي قرصنة . ١٤- تستطيع المنظمة مكافحة الخروقات الامنية التي تتعرض لها في مجال المعلوماتية . ١٥- هناك قسم او وحدة مختصة بأمنية نظام المعلومات . ١٦- هناك قدرة على كشف الخروقات الامنية .			
	ب- مستوى المساهمة:- ١٧- توجد متطلبات تسهل الحماية لامنية نظام المعلومات . ١٨- تستخدم برامج الجدار الناري لتوفير الحماية . ١٩- تستخدم كلمة السر للحماية . ٢٠- تستخدم برامج لمكافحة الفيروسات التي قد يتعرض لها نظام المعلومات ٢١- لغرض القيام بتقييم القياسات الامنية لانظمة المعلومات يجري تطوير افضل الممارسات للحد من عمليات القرصنة والسطو.			
	ج-نظام المخاطرالدقيقة: ٢٢- يمكن قياس النظام الامني المستخدم بنسبة مئوية. ٢٣- نتائج الاداء تستند على اهداف القياس الامني لنظم المعلومات والتي تهدف الى الحماية والسرية.			
	معاملات نظام التنبيه للمخاطر: **أ- نظام المخاطر الوقتية:** ٢٤- هناك كشف للمخاطر على نظام المعلومات المستهدف . ٢٥ - يتم تخصيص موارد كافية لمواجهة المخاطر الامنية .			
	٢٦- توجد مصداقية في التقارير المستخرجة من القياسات الامنية. ٢٧- يمتلك المصرف النماذج التي يستطيع الاعتماد عليها في قياس شدة المخاطر.			
	٢٨- لدى المصرف متخصصين لمواجهة المخاطر الامنية التي يتعرض لها نظام المعلومات . ٢٩ - يوجد فريق لامن نظم المعلومات يتحمل مسؤولية سياسات أمن وبرامج أنظمة المعلومات.			
	ب- نظام المخاطر البيئية :- ٣٠ – يجري المصرف تدقيق وصيانة لانظمة معلوماته . ٣١ - هناك امكانية لاسترجاع المعلومات التي قد يتم خرقه.			

ملحق (٢) المصطلحات المهمة المستخدمة في البحث

نظـام التنبيـه عنـد التعـرض للمخـاطر وتسجيلها	CVSS = Common Vulnerability Scoring System
النتيجة الاساسية	BS = Base Score
متجه الوصول للمعلومة	AV = Access Vector
تعقيد الوصول للمعلومة	AC = Access Complexity
المصداقية والتوثيق	A= Authentic Caution
تاثير السرية	CI = Confidentiality
قاعدة التاثير	IB = Impact bias
تاثير السلامة	II = Integrity Impact
تاثير الامكانية	AI = Availability Impact
النتيجة الوقتية	TS = Temporal score
قابلية الانجاز	E = Exploitability
مستوى المعالجة	RL = Remediation Level
ثقة القرير	RC = Report Confidence
نتيجة البيئة	ES = Environmental Score
نتيجة الوقت	TS = Temporal Score
الاضرار المحتملة	CDP = Collateral Damage
توزيع(المساهمة) الهدف	TD = Target Distribution

ملحق (٣) اسماء السادة المحكمين لاستمارة الفحص

الاسم	الموقع الوظيفي
١- ا.م .د صلاح الدين عواد الكبيسي	استاذ مساعد /كلية الادارة والاقتصاد / جامعة بغداد
٢- أ .م.د اياد عبد الرحيم	استاذ مساعد /الكلية التقنية / رئيس قسم
٣- ا.م .د انتصار عباس	استاذ مساعد /كلية الادارة والاقتصاد / جامعة بغداد
٤- د. عبد الله حكمت عبو	مدرس وزارة التعليم العالي والبحث العلمي
٥- السيد مروان عبد الحميد	مـدرس / كليـة الادارة والاقتصـاد/ مـدير مركـز الحاسبة اللاكترونية

ملحق (٤) اسماء السادة الخبراء من موظفي المصرف

الاسماء	المنصب الوظيفي
١- السيد هاشم عباس جاسم	مدير المصرف
٢- السيد نجم مجدي فتحي	معاون المدير
٣- الست ندى علي سعد	مسؤولة قسم المعلوماتية
٤-الست الاء علي شهاب	مسؤولة برامج الحاسوب
٥- الست فاتن فؤاد	رئيس مرمجين
٦- الست رباب عبد الرضا	رئيس مبرمجين