دور الأمن المعلوماتي في تفعيل نشاط الصيرفة الالكترونية

أ/ نور الدين بـــربار[1]

أ / محمد هشام قلمين[2]

الملخص:

الهدف من هذه الورقة البحثية هو تسليط الضوء على قضية مهمة جدا تتعلق بالأمن المعلوماتي ودوره في تفعيل نشاط التجارة الالكترونية عموما و الصيرفة الالكترونية خصوصا لاسيما مع بروز الفجوة الرقمية ليست بين الدول فحسب بل بين مدى استخدام وسائل تكنولوجيا المعلومات والاتصال في المصرف في حد ذاته ومدى مواكبته لما يحدث داخل أي منظومة مصرفية ، لذا ستبحث هذه الدراسة في تحليل ودراسة مختلف العوامل التي تعمل على إرساء منظومة مصرفية الكترونية تستجيب للمقاييس والموصفات المتعلقة بضمان السرية والأمن لمختلف المعاملات والمعلومات الالكترونية .

الكلمات الدالة : الأمن المعلوماتي ، الصيرفة الالكترونية ، المعلوماتية.

Résumé:

le objectif du cette recherche c'est abordé un sujet très important, qui concerne la sécurité du l'information ou le "Cyber sécurité ", et son rôle dans E-commerce, et E-banking, surtout avec la fracture numérique pas seulement entre les pays , mais même entre les banques et leurs l'utilisation des technologie d'information et communication, et a quel point la banque et a jour avec les autres systèmes bancaires, dans cette recherche on vas analysé les éléments qui nous construire un E-systeme bancaire, compatible avec les normes et les spécifications qui correspond la garantie du la confidentialité et la sécurité du toutes les opérations et les informations des banques.

Mots clés: Cyber sécurité, E-banking, l'informatique.

[1] باحث بمخبر تحديات النظام الضريبي الجزائري في ظل التحولات الاقتصادية بجامعة البليدة 02 ومسجل لتحضير الدكتوراه بقسم العلوم الاقتصادية ، تخصص المالية والبنوك بجامعة البليدة 02 ، مفتش رئيسي للمنافسة والتحقيقات الاقتصادية لدى مديرية التجارة بولاية المدية ، رقم الهاتف : 73 12 96 56 5 0، البريد الالكتروني : berberd2012@yahoo.fr. ، Berbernourd06@hotmail.fr.

[2] باحث بمخبر تسيير الجماعات المحلية ودورها في تحقيق التنمية بجامعة البليدة 02 ، ومسجل لتحضير الدكتوراه بقسم العلوم الاقتصادية ، تخصص المالية والبنوك بجامعة البليدة 02 ، أستاذ معيد بجامعة البليدة 02 ، رقم الهاتف:61 14 39 95 7 0 البريد الالكتروني : mohamedhichem2013@yahoo.fr.

مقدمة:

شهد الاقتصاد العالمي خلال السنوات الأخيرة تغيرات جذرية عميقة نتيجة للعولمة التي قربت المسافات وكسرت الحدود وقلصت الوقت وازدادت هذه التغيرات مع بروز تكنولوجيا المعلومات والاتصال وانسياب تطبيقاتها في جميع جوانب الحياة بما في ذلك الجانب الاقتصادي وهذا بغية توفير خدمات ذات جودة عالية وتكاليف معقولة يمكنها أن تحقق للمؤسسات أكبر قدر ممكن من الأرباح وتحافظ على بقائها في السوق ومن ضمن القطاعات التي عززت استثماراتها في وسائل تكنولوجيا المعلومات نجد البنوك والمؤسسات المالية نظرا لامتلاكها لمبالغ مالية تؤهلها لتسويق خدماتها في ظل الاقتصاد الافتراضي الذي فرض نفسه ولم يفسح المجال للاختيار بل أصبح ضرورة ملحة في ظل المنافسة القوية.

وتماشيا مع التطور التكنولوجي وبروز البنوك الالكترونية الى حيز الوجود اصطدمت هذه البنوك بالمشاكل التكنولوجية وعلى رأسها مشكلة القرصنة التي تعتبر أخطر جريمة اقتصادية تمس الحسابات المصرفية والتي تؤثر على نشاط المصرف وسمعته والتي تؤدي الى انعدام الثقة فيه مما يهدد بقاءه في السوق ، واستجابة للواقع الجديد ونتيجة للمشاكل المتكررة التي ظهرت الى حيز الوجود مع التطبيقات المتكررة لنشاط المصارف الالكترونية أصبح من الضروري البحث عن الحلول للمشاكل التي تعترض نشاط الصيرفة الالكترونية من خلال اتخاذ مختلف التدابير الرامية للحفاظ على المعلومات والأجهزة والبرمجيات من كل عملية قرصنة قد تحدث بصفة غير قانونية وهو ما أصطلح على تسميته بتوفير الأمن المعلوماتي الذي يسمح ببقاء البنك في ظل المنافسة القوية ، وفي هذا السياق ستحاول هذه الدراسة تحليل الاشكالية التالية : **مدى قدرة الأمن المعلوماتي في إعطاء الجودة والتميز لمنتجات الصيرفة الالكترونية؟**

ولدراسة وتحليل هذه الإشكالية نبني دراستنا على الفرضية التالية : **جودة منتجات الصيرفة الالكترونية تتوقف على فاعلية الأنظمة المعلوماتية التي تضمن سرية الخدمة وإتاحتها في الوقت المناسب لطالبيها.**

أهمية الدراسة: تكمن أهمية الدراسة في ابراز مكانة الأمن المعلوماتي في ارساء نشاط الصيرفة الالكترونية بالنظر لإتاحته لخصائص الخدمة المصرفية من جهة وإعطائها التميز من جهة أخرى ، وهذا التميز نابع من طبيعة التقنية المستخدمة ألا وهي وسائل تكنولوجيا المعلومات والاتصال التي أصبحت وسيلة العصر في مختلف مجالات الحياة .

ولمعالجة الاشكالية السابقة قسمنا هذه الورقة البحثية الى ثلاثة محاور أساسية كما يلي: .

المحور الأول : عموميات حول الصيرفة الالكترونية والمصارف الالكترونية.

المحور الثاني :الأمن المعلوماتي.

المحور الثالث : الأمن المعلوماتي ودوره في تفعيل نشاط الصيرفة الالكترونية.

وفي ما يلي عرض للخطوط العريضة لهذه الورقة البحثية:

المحور الأول : عموميات حول الصيرفة الالكترونية والمصارف الالكترونية:

تماشيا مع وتيرة التطور التكنولوجي الذي شهده العالم اتجهت البنوك والمؤسسات المالية الى استغلال هذه التكنولوجيا في طرح مختلف أوعيتها ومنافذها التمويلية تسهيلا للعملية التنموية وتخفيضا للتكاليف ومواجهة للمنافسة الكبيرة التي أصبحت تميز القطاع المالي ، وفي هذا السياق سنحاول عرض بعض المفاهيم العامة المتعلقة بالبنوك الالكترونية والصيرفة الالكترونية.

أولا: التعريف المصارف الالكترونية: من ضمن التعاريف التي أعطيت للمصارف الالكترونية نجد:

المصارف الالكترونية (E-Banking) : تعني التسليم التلقائي لمنتجات وخدمات المصارف الحديثة والتقليدية إلى يد العميل أو المستثمر بصورة مباشرة عبر الطريق الالكتروني وقنوات الاتصال التفاعلية ، ويستخدم تعبير المصارف الالكترونية أو مصارف الانترنت بوصفه تعبيراً متطوراً وشاملاً للمفاهيم التي ظهرت في العقد الأخير من القرن الماضي كمفهوم الخدمات المالية عن بعد أو المصارف الالكترونية عن بعد أو المصرف المنزلي أو الخدمات المالية الذاتية وجميعها تعبيرات تتصل بقيام الزبائن بإدارة حساباتهم وإنجاز أعمالهم المتصلة بالمصرف عن طريق المنزل أو المكتب أو أي مكان أخر وفي الوقت الذي يريد الزبون ، ويمكن التعبير عنها (الخدمة المالية في كل وقت ومن أي مكان) ، وقد كان الزبون عادةً يتصل بحساباته لدى المصرف ويتمكن من الدخول إليها وإجراء ما تتيحه له الخدمة عن طريق خط خاص [i].

وتطور هذا المفهوم مع شيوع الانترنت حيث أصبح بإمكان الزبائن الدخول من خلال الاشتراك العام عبر الانترنت ، لكن بقيت فكرة الخدمة المالية عن بعد تقوم على أساس وجود البرمجيات المناسبة داخل نظام حاسوب الزبون ، بمعنى أن المصرف يزود جهاز العميل (الحاسوب الشخصي) بحزمة البرمجيات ، إما مجاناً أو لقاء رسوم مالية ، وهذهِ تمكنه من تنفيذ عمليات معينه عن بعد (المصرف المنزلي) ، أو كان العميل يحصل على حزمة البرمجيات اللازمة عبر شرائها من الجهات المزودة ، وعرفت هذهِ الحزم باسم برمجيات الإدارة المالية مثل حزمة (Microsoft's Money) وحزمة برمجيات (Quicken Intuits) وحزمة(Mecca's Managing Your Money) وغيرها ، وهذا المفهوم للخدمات المالية عن بعد هو الذي يعبر عنه واقعياً بمصرف الحاسوب الشخصي (PC Banking) وهو مفهوم وشكل قائم ولا يزال الأكثر شيوعاً في عالم العمل المصرفي الالكتروني .

ثانيا : مراحل تطور الصيرفة الالكترونية : حصل في العمل المصرفي بين عام 1950 وعام 1970 ثلاث تطورات مهمة تمثلت في دخول المهنيين الى القطاع المصرفي مع أعقاب نهاية الحرب العالمية الأولى ، ومن ثم مرحلة تنامي دور

التكنولوجيا وكمرحلة أخيرة دخول ثقافة التسويق والبيع المتقدمة **مراحل استخدام تكنولوجيا المعلومات في العمل المصرفي** : تم استخدام تكنولوجيا المعلومات في المصارف عبر ستة مراحل أساسية شملت :

1/2– مرحلة الدخول : وهي المرحلة التي دخلت فيها التكنولوجيا إلى أعمال المصارف حيث عمل الأخصائيون في شؤون المصارف على إيجاد حلول للأعمال المكتبية من خلال المنافذ والتطبيقات التكنولوجية " إيجاد الحلول التكنولوجية لمشاكل الأعمال المصرفية الخلفية " مثل مشكلات التأخير في إعداد التقارير المالية والتقارير المحاسبية ولم يكن هناك تدخل مباشر من قبل الإدارات الوسطى والعليا التنفيذية سواء في الحلول المقترحة أو في كلفتها ، فكان المهم هو حل المشاكل المتعلقة بالعمل المصرفي.

2/2 –مرحلة تعميم الوعي بالتكنولوجيا: وهي المرحلة التي بدأت بتعميم الوعي بالتكنولوجيا على كافة العاملين بالمصرف من خلال برامج تدريب تغلب عليها التقنية على حساب المعرفة بالأعمال ، وكانت مرحلة تحضير أوسع لدخول التكنولوجيا وتميزت هذه المرحلة بعدم وجود تدخل مباشرة من قبل الإدارات الوسطى والعليا.

3/2 – مرحلة دخول الاتصالات والتوفير الفوري لخدمات العملاء :وتميزت هذه المرحلة بالتكاليف العالية ، حيث بدأ اهتمام الإدارات العليا بالتكنولوجيا.

4/2– مرحلة الضبط أو السيطرة على التكاليف: وهي مرحلة ضبط الاستثمار في التكنولوجيا ، وعمدت هذه الإدارات إلى الاستعانة بأخصائيين واستشاريين في شؤون التكنولوجيا لمساعدتهم في ضبط التكاليف.

5/2– مرحلة اعتبار التكنولوجيا أصلا كباقي أصول المصرف : بالتالي يجب أن يجني هذا الأصل مردودا كباقي الأصول ، وهنا بدأت مرحلة إدارة التكنولوجيا.

5/2 –مرحلة اعتبار التكنولوجيا عملا ضمن أعمال المصرف : وهي المرحلة التي بدأت فيها الإدارة الإستراتيجية للتكنولوجيا ، والتي ارتكزت على تفعيل الإنتاجية على الصعيد الداخلي ، تحسين الضبط على الصعيد العملي ، وتسويق التكنولوجيا .

ثالثا: أنماط المصارف الالكترونية : هناك الكثير من المفاهيم والمستويات الخاطئة في تحديد المراد بالمصارف الالكترونية ، فبعض المصارف أنشأت موقعاً تعريفياً لخدماتها وفروعها واكتفت بذلك ،وطبعاً لا يدخل هذا ضمن مفهوم المصارف الالكترونية ، وقد لوحظ أن بعض المصارف العربية صممت مواقعها منذ فترة طويلة وما تزال على ذات المحتوى دون تطوير لمواردها التعريفية ، وكأن المراد هو مجرد الوجود على شبكة الانترنيت وليس تقديم خدمة مالية الكترونية متكاملة ، فإذا كان للبنك موقعاً على شبكة الانترنيت فهذا لا يعني أنه مصرف الكتروني ، وسيظل معيار تحديد المصرف الالكتروني مثار تساؤل في بيئتنا العربية إلى أن يتم تشريعياً تحديد معيار منضبط في هذا الحقل [ii]،

ووفقاً للدراسات العالمية وتحديداً لدراسات جهات الإشراف والرقابة الأمريكية والأوربية ، فان هناك ثلاث صوراً أساسيه لأنماط مواقع المصارف الالكترونية على شبكة الانترنيت وهي :

1/3- المواقع المعلوماتية (Informational Websites) : هو المستوى الأساسي للمصارف الالكترونية أو ما يمكن تسميته بصورة الحد الأدنى من النشاط الالكتروني المصرفي ، ومن خلاله فإن المصرف يقدم معلومات عن برامجه ومنتجاته وخدماته المصرفية ، ويشمل هذا نوعين من مواقع المعلومات وهي:

- مواقع المعلومات الأساسية التي لا توفر سوى معلومات عن منتجات وخدمات المصارف المقدمة إلى زبائن المصرف والناس كافة.

- مواقع المعلومات الالكترونية المعلوماتية والتي تمكن الزبائن من الاطلاع على المعلومات العامة عن المؤسسة المالية المعنية والخدمات التي تقدمها ومنتجاتها ، إضافة إلى إمكانية السؤال عن الرصيد ، ويجب أن تتحمل الشركة صاحبة الموقع المسؤولية القانونية اتجاه الزبائن في حالة عدم صحة أي من المعلومات المعروضة في الموقع من منتجات الشركة وخدماتها والأسعار التي يجري التعامل بها ، وأن تتحمل الشركة المسؤولية القانونية إذا قام موقعها بدورٍ ما في نشر فيروسات أو أي نوع من البرامج التخريبية إلى الحواسيب التي تتصل بالموقع .

يجب ألا يكون هناك أي احتمال للولوج إلى المعلومات المالية السرية للشركة أو لزبائنها ، ويعتبر الموقع المعلوماتي للمصرف الالكتروني شكلاً من أشكال الدعاية الإعلامية للمصرف ، ولا يمكن للمصرف تقديم أي نوع من الخدمات [iii].

2/3- المواقع التفاعلية أو الاتصالية:(Communicative Websites) :يسمح الموقع بنوع ما من التبادل الاتصالي بين المصرف وعملائه كالبريد الالكتروني وتعبئة طلبات أو نماذج على الخط أو تعديل معلومات القيود والحسابات ويشمل هذا الموقع نوعين وهما :

- مواقع المعلومات البسيطة التي تسمح لزبائن المصرف أن يطلبوا خدمات متعددة ويطرحوا بعض الأسئلة عن أرصدة حساباتهم وما إلى ذلك ، دون السماح بأي مداولات على أرصدة حساباتهم.

- الموقع التفاعلي الذي يسمح بنوع ما من التبادل المعلوماتي بين المصرف و زبائنه بواسطة البريد الالكتروني مثلاً ، وتعبئة طلبات أو نماذج على نحو مباشر على الخط ، أو تعديل معلومات القيود والحسابات .

3/3- مواقع التعاملات (Transactional Websites) :وهو المستوى الذي يمكن القول أن المصرف فيه يمارس خدماته وأنشطته في بيئة الكترونية ، حيث تشمل هذهِ الصور السماح للزبون بالوصول إلى حساباته

وإداراتها وإجراء الدفعات النقدية والوفاء بقيمة الفواتير وإجراء كافة الخدمات الاستعلامية وإجراء الحوالات بين حساباته داخل المصرف أو مع جهات خارجية ، ويشمل هذا الموقع نوعين وهما :

– مواقع المبادلات المتقدمة والتي تسمح للزبائن بأن يحركوا حساباتهم إلكترونياً ، وأن يدفعوا الفواتير ويقوموا بكافة المداولات المصرفية مباشرة.

– الموقع التبادلي الذي يتيح لزبائنه إمكانية إجراء التعاملات المالية التي تتضمن فحص الحسابات المالية ، وعمليات التحويل المالية الكبرى التي تجري لأهداف تجاريه ، وذلك بشراء الخدمات التي تمكن الزبون من التعامل مع المؤسسة المالية لإجراء ما يناسب عمله وتتنوع الخدمات التي تقدمها للشركات المالية بتنوع العمليات التي سيقوم بها الزبائن ، ويجب على هذهِ المواقع أن تأخذ بعين الاعتبار النقاط التالية :

– الحفاظ على سرية المعلومات الخاصة بالعملاء عند تبادل البيانات عن طريق موقع المصرف الالكتروني .

– الاستيقان: ويهدف إلى التحقق من هوية العملاء الجدد ، واستيقان العملاء الموجودين الذين يحاولون استخدام خدمات المصرف الالكتروني .

– المسؤولية القانونية في حالة القيام بأي عملية مناقلة غير قانونية .

– التقليل من عمليات الاحتيال في حالة عدم التحقق من هوية الشخص أو المؤسسة التي تحاول إنشاء حساب جديد أو فتح اعتماد عن طريق شبكة الانترنيت ، وذلك بعدم السماح لها بالقيام بذلك إلا بعد الحصول على إثباتات معينة.

– احتمال اختراق الأنظمة والقوانين الخاصة بحماية الخصوصية للعميل من قبل جهات معينة ، عند الشك في حالات غسيل الأموال أو تمويل المنظمات الإرهابية.

– تحمل المصرف المسؤولية القانونية عند الإخفاق في تحويل دفعات مالية من العميل إلى طرف ثالث غير المصرف كما هو محدد تماما أو التأخير في التحويل ، أو حصول أي عملية قرصنة على حساب العميل خلال عملية التحويل أو التخزين[iv] .

رابعا : متطلبات قيام المصارف الالكترونية : يتطلب إنشاء مصارف الكترونية ما يلي:

1/4– البنية التحتية التقنية : يقف في مقدمة متطلبات قيام المصارف الالكترونية البنية التحتية التقنية ، والبنية التحتية التقنية للبنوك الالكترونية لا يمكن أن تكون معزولة عن البنية التحتية للدولة في مجال الاتصالات ، كون أن المصارف الالكترونية تنشط في بيئة الأعمال الافتراضية والمتطلب الرئيسي لضمان أعمال الكترونية ناجحة بل وضمان دخول آمن وسلس لعصر المعلومات يتمثل في كفاءة قطاع الاتصالات من خلال سلامة البنية التحتية وملائمة

أسعار الربط بشبكة الانترنت ، فلا يمكن قيام البنوك الالكترونية في بيئة عدد المشتركين بشبكة الانترنيت قليل فمسألة توافر شبكة الانترنت وملائمة تكاليفها تمثل أهم تحد أمام بناء المصارف الالكترونية وتتطلب تدخلا جماعيا لرفع كل قيود تعترض تزايد استخدام الشبكة كما أن فعالية وسلامة بنى الاتصالات تقوم على سلامة التنظيم الاستثماري ، ودقة المعايير وتواؤمها الدولي ، وكفاءة وفعالية التنظيم القانوني لقطاع الاتصالات ، وبقدر ما تسود معايير التعامل السليم مع هذه العناصر يتحقق توفير أهم دعامة للتجارة الالكترونية ، بل وللبناء القوي للتعامل مع عصر المعلومات[v] .

من عناصر البنية التحتية لقطاع الاتصالات نجد مدى توافر الأجهزة والبرمجيات والكفاءات البشرية المدربة والوظائف الاحترافية ، وهذه دعامة للوجود والاستمرارية والمنافسة ، ولم يعد المال وحده المتطلب الرئيس ، بل استراتيجيات التواؤم مع المتطلبات وسلامة البرامج والنظم المطبقة لضمان تعميم التقنية بصورة منظمة وفاعلة وضمان الاستخدام الأمثل والسليم لوسائل التقنية.

أما عن عناصر إستراتيجية البناء التحتي في حقل الاتصالات وتقنية المعلومات ، فإننا نرى أنها تتمثل بتحديد أولويات وأغراض تطوير سوق الاتصالات في الدولة ، ومواءمة هدف الدخول للأسواق العالمية مع احتياجات التطوير التقنية للشركات الخاصة ، والسياسات التسويقية والخدمية والتنظيمية المتعين اعتمادها لضمان المنافسة في سوق الاتصالات ولضمان جذب الاستثمارات في هذا القطاع ، وتنظيم الالتزامات لمقدمي الخدمات مع تحديد معايير ومواصفات الخدمة المميزة ، وفي مقدمتها معايير امن وسلامة تبادل المعلومات وسريتها وخصوصية المشتركين ، وتوفير الإطار القانوني الواضح الذي يحدد الالتزامات على أطراف العلاقة ، وأخيرا تحديد نطاق التدخل الحكومي وتحديد أولويات الدعم وما يتعين أن يكون محلا للتشجيع الاستثماري من قبل الدولة.

وتوفر البنى التحتية العامة يبقى غير كاف دون مشاريع بناء بنى تحتية خاصة بالمنشآت المصرفية ، وهو اتجاه تعمل عليه المصارف بجدية ، ونكتفي في هذا المقام بالقول أن عنصر التميز هو إدراك مستقبل تطور التقنية وتوفير بنى وحلول برمجية تتيح مواصلة التعامل مع التطورات الجديدة ، فتقنية حصرية تعني أداءا ضيقا والمسألة ليست مسألة أموال وإنما خطط سليمة وكفاءات إدارية مميزة ترى المستقبل أكثر مما ترى الحاضر.[vi] .

2/4/– الكفاءة الأدائية المتفقة مع عصر التقنية :هذه الكفاءة القائمة على فهم احتياجات الأداء والتواصل التأهيلي والتدريبي ، والاهم من ذلك أن تمتد كفاءة الأداء إلى كافة الوظائف الفنية والمالية والتسويقية والقانونية والاستشارية والإدارية المتصلة بالنشاط المصرفي الالكتروني[vii].

3/4– التطوير والاستمرارية والتفاعلية مع المستجدات : ويتقدم عنصر (التطوير والاستمرارية والتنوعية) على العديد من عناصر متطلبات بناء المصارف الالكترونية وتميزها ، فالجمود وانتظار الآخرين لا يتفق مع التقاط فرص التميز ، ويلاحظ الباحث العربي أن المصارف العربية لا تتجه دائما نحو الريادية في اقتحام الجديد ، إنها تنتظر أداء الآخرين ، وربما يكون المبرر الخشية على أموال المساهمين واجتياز المخاطر ، وهو أمر هام وضروري ، لكنه ليس مانعا من الريادية ، وبنفس القدر لا تعني الريادية في اقتحام الجديد التسرع في التخطيط للتعامل مع الجديد وإعداد العدة لكنها حتما تتطلب السرعة في انجاز ذلك .

4/4– التفاعل مع متغيرات الوسائل والاستراتيجيات الفنية والإدارية والمالية : والتفاعلية لا تكون في التعامل مع الجديد فقط أو مع البنى التقنية فقط وإنما مع الأفكار والنظريات الحديثة في حقول الأداء الفني والتسويقي والمالي والخدمي ، تلك الأفكار التي تنشئ نتيجة لتفكير الإبداعي وليس وليدة لتفكير النمطي .

5/4– الرقابة التقييمية الحيادية : إن واحدا من عناصر النجاح الارتكان للتقييم الموضوعي ، ومن هنا أقامت غالبية مواقع المصارف الالكترونية جهات مشورة في تخصصات التقنية والتسويق والقانون والنشر الالكتروني لتقييم فعالية وأداء مواقعها ، ويتعين أن نحذر من مصيدة الارتكان إلى عدد زائري الموقع كمؤشر على النجاح ، إذ يسود فهم عام أن كثرة زيارة الموقع دليل نجاح الموقع ، لكنه ليس كذلك دائما وان كان مؤشرا حقيقيا على سلامة وضع الموقع على محركات البحث وسلامة الخطط الدعائية والترويجية.

المحور الثاني: الأمن المعلوماتي:

تشكل المعلومات المصدر الأساسي الذي يتيح للمنظمات اتخاذ القرارات المناسبة ويمكنها من تأدية مهامها ، إذ أن نوع المعلومات و كميتها و طريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة و عليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها و تداولها و وضع السبل الكفيلة بحيازتها ، لذا فإن المشكلة التي يجب أخذها بالحسبان هو توفير الحماية اللازمة للمعلومات و إبعادها عن الاستخدام غير المشروع لها .

أولا : التعريف بالأمن المعلوماتي"Information Security " :من ضمن المفاهيم التي أعطيت للأمن المعلوماتي نجد:

هو مجموعة من الإجراءات و التدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات و الأجهزة و البرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال ، والبعض قد عرفه بأنه الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضياع و التلف أو من مخاطر الاستخدام غير

الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية ، كما عرف بأنه مجموعة من التدابير الوقائية المستخدمة في المجالين الإداري و الفني لحماية مصادر البيانات من أجهزة و برمجيات و بيانات من التجاوزات أو التداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل أو الإجراءات الخاطئة المستخدمة من قبل إدارة المصادر المعلوماتية ، فضلا عن إجراءات مواجهة الأخطار الناتجة عن الكوارث الطبيعية المحتملة التي تؤدي إلى فقدان بعض المصادر كليا أو جزئيا ، و من ثم التأثير على نوع و مستوى الخدمة المقدمة [viii].

فمن خلال كل ما سبق يمكن أن نعرف الأمن المعلوماتي بأنه ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزنة في أجهزة الحواسيب والأجهزة الملحقة و شبكات الاتصالات و التصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزنة أو تلك التي ترمي إلى نقل أو تغيير أو تخريب تلك المعلومات .

ثانيا: العناصر الأساسية لنظام الأمن المعلوماتي :إن النظام الأمني الفعال يجب أن يشمل جميع العناصر ذات الصلة بنظام المعلومات المحوسبة و يمكن تحديد هذه العناصر بما يلي [ix]:

1/2– منظومة الأجهزة الإلكترونية و ملحقاتها : إن أجهزة الحواسيب تتطور بشكل كبير جدا بالمقابل هناك تتطور في مجال السبل المستخدمة لاختراقها مما يتطلب تطوير القابليات و المهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب و العبث المقصود في الأجهزة أو غير المقصود .

2/2– الأفراد العاملين في أقسام المعلومات : يلعب الفرد دورا أساسيا و مهما في مجال أمن المعلومات و الحواسيب و له تأثير فعال في أداء عمل الحواسيب بجانبيه الإيجابي و السلبي ، فهو عامل مؤثر في حماية الحواسيب و المعلومات و لكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة و سرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير ، فمن متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين و وضع تعليمات واضحة لاختيارهم و ذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد إضافة إلى وضع الخطط لزيادة الحس الأمني و الحصانة من التخريب ، كما يتطلب الأمر المراجعة الدورية للتدقيق في الشخصية و السلوكية للأفراد العاملين من وقت لآخر و ربما يتم تغيير مواقع عملهم و محاولة عدم احتكار المهام على موظفين محدودين .

3/2– البرمجيات المستخدمة في تشغيل النظام : تعتبر البرمجيات من المكونات غير المادية و عنصر أساسي في نجاح استخدام النظام ، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية و يمكن أن تحقق حماية للبرامج و طرق حفظ كلمات السر و طريقة إدارة نظام التشغيل و أنظمة الاتصالات ، فأمن البرمجيات يتطلب أن يؤخذ هذا الأمر بعين الاعتبار عند تصميم النظام و كتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح و

العوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها و تمنع أي شخص من إمكانية التلاعب والدخول إلى النظام و ذلك من خلال تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها ، و محاولة التمييز بين اللذين يحق لهم الإطلاع و حسب كلمات السر الموضوعة ، و هناك أسلوبان للتمييز إما عن طريق البرمجيات أو استخدام الأجهزة المشفرة.

4/2– شبكة تناقل المعلومات :تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطور في مجال الاتصالات التي سمحت بتسهيل عملية الاتصال من خلال اتاحة عملية استخدام وتبادل الملفات الكترونيا ، لكن تماشيا مع هذا التطور ظهرت الى حيز الوجود العديد من المشاكل ومن ضمنها عملية سرقة المعلومات أو تدميرها سواء من الداخل كاستخدام الفيروسات أو من خلال الدخول عبر منظومات الاتصال المختلفة لذلك لا بد من وضع إجراءات حماية و ضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات و توفير الأجهزة الخاصة بالفحص ، كما أن نظم التشغيل المستخدمة و المسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة و قدرة عالية على الكشف عن التسلل إلى الشبكة و ذلك من خلال تصميم نظم محمية بإقفال معقد أو عن طريق المشفرات و ربطها بخطوط الاتصال و التي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة و معدات لغرض تحفيز تناقل المعلومات أو الملفات [x].

5/2– مواقع منظومة الأجهزة الإلكترونية و ملحقاتها : يجب أن تعطى أهمية للمواقع و الأبنية التي يحوي أجهزة الحواسيب و ملحقاتها ، و حسب طبيعة المنظومات و التطبيقات المستخدمة يتم اتخاذ الإجراءات الاحترازية لحماية الموقع و تحصينه من أي تخريب أو سطو و حمايته من الحريق أو تسرب المياه و الفيضانات ، و محاولة إدامة مصدر القدرة الكهربائية و انتظامها و تحديد أساليب و إجراءات التفتيش و التحقق من هوية الأفراد الداخلين و الخارجين من الموقع و عمل سجل لذلك .

ثالثا :المخاطر التي تواجه الأمن المعلوماتي: لقد أصبح اختراق أنظمة المعلومات و نظم الشبكات و المواقع المعلوماتية خطراً يقلق العديد من المنظمات في السنوات الأخيرة و مع مرور الزمن نجد أنه على الرغم من سبل الحماية التي تتبعها المنظمات ، إلى أن هناك ارتفاعا واضحا في معدل الاختراقات مع تنوع الوسائل المستخدمة في الاختراق أما عن طبيعة الأخطار التي يمكن أن تواجهها نظم المعلومات فهي عديدة ، فالبعض منها قد يكون مقصود كسرقة المعلومات أو إدخال الفيروسات و غيرها و هي الأشد ضررا على نظم المعلومات و يكون مصدرها أحيانا من داخل أو خارج المنظمة [xi] ، و قد يصعب أحيانا التنبؤ بالدوافع العديدة للأشخاص الذين يقومون بها ، أما البعض الآخر

فقد يكون غير مقصود كالأخطاء البشرية و الكوارث الطبيعية و يمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات إلى ثلاث فئات :

1/3– الأخطاء البشرية :و هي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام ، أو في عمليات تحديد الصلاحيات للمستخدمين ، و تشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن و سلامة نظم المعلومات في المنظمات .

2/3– الأخطار البيئية :و هذه تشمل الزلازل و العواصف و الفيضانات و الأعاصير و المشاكل المتعلقة بأعطاب التيار الكهربائي و الحرائق إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف و التبريد و غيرها ، و تؤدي هذه الأخطار إلى تعطل عمل هذه التجهيزات و توقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة و استرداد البرمجيات و قواعد البيانات .

3/3– الجرائم المحوسبة : تمثل هذه تحديا كبيرا لإدارة نظم المعلومات لما تسببه من خسارة كبيرة و بشكل عام يتم التمييز بين ثلاثة مستويات للجرائم المحوسبة و هي :

1/3/3– سوء الاستخدام لجهاز الحاسوب : و هو الاستخدام المقصود الذي يمكن أن يسبب خسارة للمنظمة أو تخريب لأجهزتها بشكل منظم .

2/3/3– الجريمة المحوسبة : و هي عبارة عن سوء استخدام لأجهزة الحاسوب بشكل غير قانوني يؤدي إلى ارتكاب جريمة يعاقب عليها القانون خاصة بجرائم الحاسوب .

3/3/3– الجرائم المتعلقة بالحواسيب : و هي الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة .

و يمكن أن تتم الجرائم المحوسبة سواء من قبل أشخاص خارج المنظمة يقومون باختراق نظام الحاسوب (غالبا من خلال الشبكات) أو من قبل أشخاص داخل المنظمة يملكون صلاحيات الدخول إلى النظام و لكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة ، و تشير الدراسات التي أجرتها دائرة المحاسبة العامة و شركة Orkand للاستشارات إلى أن الخسائر الناتجة عن جرائم الكمبيوتر تقدر بحدود 1.5 مليون دولار لشركات المصارف المحوسبة في الولايات المتحدة الأمريكية ، و من ناحية أخرى يقدر المركز الوطني لبيانات جرائم الحاسوب في لوس أنجلوس بأن 70% من جرائم الكمبيوتر المسجلة حدثت من الداخل ، أي من قبل من يعملون داخل المنظمات ، فتزايد جرائم الحاسوب بصورة واضحة أصبح يشكل تحديا خطيرا يواجه الإدارات العليا عموما و إدارة نظم المعلومات على وجه الخصوص[xii] .

رابعا: الحماية من أخطار الأمن المعلوماتي : تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة و الصعبة و التي تتطلب من إدارة نظم المعلومات الكثير من الوقت و الجهد و الموارد المالية و ذلك للأسباب التالية :

- العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات.
- توزع الموارد المحوسبة على العديد من المواقع التي يمكن أن تكون أيضا متباعدة .
- وجود التجهيزات المحوسبة في عهدة أفراد عديدين في المنظمة و أحيانا خارجها .
- صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية .
- التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها.
- التأخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمنظمة إمكانية التعلم من التجربة و الخبرة المتاحة.
- تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها.

هذا و تقع مسؤولية وضع خطة الحماية للأنشطة الرئيسية على مدير نظم المعلومات في المنظمة على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق ما يلي :

- الوقاية من الأخطار غير المتعمدة .
- إعاقة أو صنع الأعمال التخريبية المتعمدة .
- اكتشاف المشاكل بشكل مبكر قدر الإمكان .
- المساعدة في تصحيح الأعطال و استرجاع النظام .

و يمكن تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات و يجب أن يركز هذا النظام على مفهوم الوقاية من الأخطار، و يمكن أن يصمم لحماية جميع مكونات النظام بما فيها التجهيزات و البرمجيات و الشبكات[xiii] .

المحور الثالث : الأمن المعلوماتي ودوره في تفعيل نشاط الصيرفة الالكترونية:

لب الدراسة التي تحاول هذه الورقة البحثية الوصول اليه هو تحليل الدور الذي يلعبه الأمن المعلوماتي في نشاط الصيرفة الالكترونية ، لذا سنحاول أن نربط بين الأمن المعلوماتي ونشاط الصيرفة الالكترونية من خلال ابراز العلاقة التكاملية بينهما حيث كلما كان الأمن المعلوماتي متوفر كلما كان نشاط الصيرفة الالكترونية أكثر فعالية لماذا لأن الأمن المعلوماتي سيضمن السرية والسرعة التي تعتبر من ضمن المبادئ الهامة التي تلتزم البنوك بها في أداء وظائفها وتنمية معاملاتها ، كما أن الاتجاه نحو المصارف الالكترونية سيجنب البنوك الالكترونية مشكلة حسن المعاملة التي قد

تنتج جراء عدم احترام موظف ما بالمصرف لأخلاقيات وضوابط المهنة ، كون أن البنوك الالكترونية المعاملة تتم بين الزبون وجهاز الحاسوب المربوط بالموقع المعلوماتي للمصرف.

أولا: مستويات ومتطلبات إرساء الأمن المعلوماتي : في حقل تحديات امن المعاملات المصرفية فإن امن المصارف الالكترونية وكذا التجارة الالكترونية جزء رئيس من امن المعلومات ونظم التقنية العالية عموما ، وتشير حصيلة دراسات امن المعلومات وما شهده هذا الحقل من تطورات على مدى الثلاثين عاما المنصرمة أن مستويات ومتطلبات الأمن الرئيسة في بيئة تقنية المعلومات تتمثل بما يلي :

– الوعي بمسائل الأمن لكافة مستويات الأداء الوظيفي من خلال الحماية المادية للتجهيزات التقنية والحماية الأدائية (استراتيجيات رقابة العمل والموظفين) الحماية التقنية الداخلية ، والحماية التقنية من المخاطر الخارجية[xiv] من خلال القاعدتين التاليتين:

1/1/ القاعدة الأولى :في حقل امن المعلومات الأمن الفاعل هو الذي يرتكز على الاحتياجات المدروسة التي تضمن الملائمة والموازنة بين محل الحماية ومصدر الخطر ونطاق الحماية وأداء النظام والكلفة ، وبالتالي فان استراتيجيات وبرامج امن المعلومات تختلف من منشأة إلى أخرى ومن بيئة إلى أخرى تبعا لطبيعة البناء التقني للنظام محل الحماية وتبعا للمعلومات محل الحماية وتبعا للآليات التقنية للعمليات محل الحماية ، إلى جانب عناصر تكامل الأداء واثر وسائل الأمن عليه وعناصر الكلفة المالية وغيرها.

2/1– القاعدة الثانية : الحماية التقنية وسيلة وقاية ودفاع وفي حالات معينة وسيلة هجوم ، كما أنه لا يمكن أن تتكامل حلقات الحماية دون الحماية القانونية من خلال النصوص التشريعية التي تحمي البنوك الالكترونية من إساءة استخدام الحواسيب والشبكات أو ما يصطلح عليه بجرائم الكمبيوتر والانترنت والاتصالات والجرائم المالية الالكترونية التي تناولنها فيما تقدم ، وبالتالي تتكامل تشريعات المصارف والتجارة الالكترونية مع النصوص القانونية لحماية المعلومات ، وبدونها يظل جسم الحماية بجناح واحد .

وإذا أردنا الوقوف في حدود مساحة العرض المتاحة على ملخص الاتجاهات الأمنية في حقل حماية البيانات في البيئة المصرفية ، والتي تتخذ أهمية بالغة بالنسبة للبنوك التي تمثل بياناتها في الحقيقة أموالا رقمية وتمثل حقوقا مالية وعناصر رئيسة في الائتمان ، نجد أن المطلوب هو وضع إستراتيجية شاملة لأمن المعلومات تتناول نظام المصرف وموقعه الافتراضي وتتناول نظم الحماية الداخلية من أنشطة إساءة الاستخدام التي قد يمارسها الموظفون المعنيون داخل المنشأة وتحديدا الجهات المعنية بالوصول إلى نظم التحكم والمعالجة والمبرمجين ، إلى جانب إستراتيجية الحماية من الاختراقات الداخلية ، وهذه الاستراتيجيات يجب أن تمتد إلى عميل المصرف لا للبنك وحده ، حتى نضمن نشاطا واعيا للتعامل

مع المعلومات وتقدير أهمية حمايتها ، ولكل إستراتيجية أركانها ومتطلباتها ومخرجاتها ، وتقييم كفاءة الإستراتيجية يقوم على مدى قدرتها على توفير مظلة امن شاملة لنظام المصرف والعميل والنظم المرتبطة بهما .

هنا يمكن التركيز على العون المكلف بعملية البرمجة للمعلومات اذ نذكر بضرورة تكوين متخصص في العمليات المصرفية والإعلام الآلي للموظفين حتى نضمن السرية والخصوصية للمعاملة المصرفية ،فإستراتيجية حماية البيانات في البيئة المصرفية تقتضي وضع حدود لتدخل كل طرف معني بالعملية المصرفية داخل النظام المعلوماتي (سواء المصرف كمستخدم أم زبائنه الذين يستخدمون التقنية للتوصل إلى موقعه الالكتروني) تحصين النظام داخليا (الحاسوب الشخصي أو محطة العمل) ، ويتم ذلك بسد الثغرات الموجودة في النظام إذ لكل نظام ثغراته ، فمثلا يوجد في نظام ويندوز الشائع خيار مشاركة في الملفات والطباعة الموجود في لوحة التحكم ضمن أيقونة الشبكة ، فهذا الخيار إذا بقي مفعلا أثناء الاتصال بالشبكة خاصة لمستخدمي وصلات الموديم الكيبلي يسمح لأي مستخدم ضمن الشبكة يتصل بالنطاق ذاته أن ينقر على أيقونة جوار شبكة الاتصال فتظهر له سواقات جهاز المستخدم ويتمكن من التعامل معها ومع الملفات الموجودة عليها ، وكذلك إلغاء خدمة عميل الشبكة (كما في عميل شبكة مايكروسفت إن لم يكن المستخدم مرتبطا بشبكة محلية عبر مزود النت، وإلغاء جميع الخيارات التي تسمح باستعمال بروتوكول من خصائص جوار الشبكة إذا كان المستخدم لا يعتمد عليه لأنه يسمح بالمشاركة بالملفات عبر المنافذ في النظام ويعد أكثر البروتوكولات المستغلة في الاختراق حسب تحليل حالات الاختراق التي قام بها مركز الرصد والاختراق لحوادث الانترنت ، وأيضا التأكد من تحديث الأنظمة المستخدمة ومتابعة ما تصدره الشركات من تعديلات لسد الثغرات التي تظهر في النظم المستخدمة ، ويمكن ذلك عبر مواقع الشركات المعنية على الانترنت مثل موقع مايكروسفت و موقع نتسكيب http://hom.netscape.com/smart update وغيرها ، إلى جانب تعديل إعدادات المصفحات أثناء زيارة الموقع غير الآمنة ، وتختلف الإعدادات باختلاف المتصفح ، لكن الغرض الرئيسي من هذه الخطوة إلغاء استقبال برمجيات أو إلغاء استقبال وإنشاء ملفات التي يمكن أن تتضمن معلومات عن كلمات السر أو غيرها مما يتم تبادلها مع الموقع الزائر ، و متابعة المواقع التي تكشف عن ثغرات البرمجيات وأنظمة التشغيل وتعالج المشاكل الأمنية مثل (http://microsoft.com/security و http://rootshell.com وhttp://www.securityfocus.com) واستخدام البرامج المضادة للفيروسات مع دوام تطويرها وتشغيل برنامجين معا إذا كان النظام يسمح بذلك دون مغالاة في إجراءات الحماية ، وإجراء عملية المسح التلقائي عند تشغيل الجهاز وتشغيل أي قرص ، والتشكيك الدوري في عمل برنامج مضاد الفيروسات وإصلاح الأعطال والأخطاء ،والحذر من برامج الدردشة والتخاطب باعتبارها تظل عاملة طيلة فترة

عمل الجهاز ، ويتعين إلغاء عملها عند الانتهاء من استخدامها ومراعاة محاذير الاستخدام ، وعدم تشغيل برامج غير معروفة المصدر والغرض مما يرد ضمن البريد الالكتروني أو مواقع الانترنت لاحتمال أن تتضمن أبواب خلفية تسهل الاختراق ، واستخدام الجدران النارية أو البرامج الشبيهة دون مغالاة بإجراءات الأمن لتأثير ذلك على الأداء ، والاهم اختيار البرامج الناجعة والمجربة ، لان بعض برامج الأمن تعد وسيلة لإضعاف الأمن وتسهيل الاختراق.[xv]

إن أهم استراتيجيات امن المعلومات توفير الكفاءات التقنية القادرة على كشف وملاحقة الاختراقات وضمان وجود فريق تدخل سريع يدرك جيدا ما يقوم به لأن أهم الاختراقات في حقل الكمبيوتر أتلفت أدلتها لخطا في عملية التعامل التقني مع النظام ، ومن جديد تظل الحماية القانونية غاية في الأهمية لأن الحماية الجنائية التي تخلق مشروعية ملاحقة أفعال الاعتداء الداخلية والخارجية على نظم الكمبيوتر وقواعد البيانات تمكن من استرداد بعض الحقوق ، اذا ما تم اثبات التهم أمام القضاء.

ثانيا: : دور أمن المعلومات في جودة منتجات المصارف الإلكترونية : من خلال تطبيق استراتيجيات الأمن المعلوماتي فإن المصارف الالكترونية سوف تضمن عدة خصائص في منتجاتها[xvi]:

1/2-**التكاملية:** وتظهر من خلال القدرة على إثبات أن المعلومات المعروضة على موقع الويب أو أن المعلومات المرسلة أو المستقبلة عبر الإنترنيت هناك جهة مسؤولة مخولة بهذا الغرض ، ويظهر من خلال تكامل الخدمة المصرفية المطلوبة .

2/2 -**عدم النكران** : من خلال القدرة على إثبات أن المشاركين في أعمال المصارف الإلكترونية لا ينكرون الأفعال التي قاموا بها تفاعلياً .

3/2- **التوثق** : من خلال القدرة على إثبات هوية الشخص أو الكيان الذي تتعامل معه على شبكة الانترنيت .

4/2- **السرية** : من خلال القدرة على إثبات أن الرسائل والمعطيات ستكون متاحة فقط للأشخاص المخولين للإطلاع عليها .

5/2- **الخصوصية** : من خلال القدرة على التحكم في استخدام المعلومات التي يقدمها المستخدم عن نفسه للمصرف أو لجهة أخرى مستفيدة.

6/2- **المُتاحية** : وهي القدرة على إثبات أن موقع المصرف الإلكتروني سيستمر بالعمل والتصرف كما هو مخطط له ، أي وفقاً لِما هو مبني من أجله.

إذن يمكن القول بأن الأمن المعلوماتي هو الضمانة الأساسية لنجاح الصيرفة الالكترونية باعتباره الآلية الأساسية التي تمكن المصارف الالكترونية من تأدية مهامها مع احترامها لمبادئ العمل المصرفي الأساسية والمتمثلة على وجه الخصوص

في السرية والسرعة ، كما أن نشاط المصارف الالكترونية يرتبط ارتباطا وثيقا بالبنية التحتية لقطاع الاتصالات في أي بلد زيادة على تكلفة استخدام شبكة الانترنت ، ومدى وجود الاطار القانوني المنظم للمعاملات الالكترونية كونه هو الألية الأساسية التي تسمح بتوسيع الأنشطة الالكترونية .

الخاتمة:

في الوقت الذي شهدت فيه وسائل تكنولوجيا المعلومات تطورا مذهلا واستخداما بالغ النظير شرعت الحكومات والدول في عملية الرقمنة لمختلف الهياكل الإدارية من خلال تبنيها لأنظمة الحكومة الالكترونية ، زيادة على توسيع الاستثمارات في وسائل تكنولوجيا المعلومات والبنية التحتية لقطاع الاتصالات وظهر ذلك في مختلف بلدان العالم من خلال التطبيقات المتزايدة لهذه التقنيات ومن ضمن القطاعات التي استثمرت في هذه التكنولوجيا القطاع المصرفي الذي أصبح يتعامل بمختلف تطبيقاتها والتي أفرزت إلى الوجود نوع جديد من المصارف أصبح يصطلح عليها بالبنوك الالكترونية التي تعتبر بمثابة تحد جديد أمام المصارف بالنظر للمشاكل التي أصبحت تعترض القطاع المصرفي خاصة تلك المتعلقة بجودة المعلومة والحفاظ على سريتها وأمنها لذلك يعتبر تطوير وسائل الحماية المعلوماتية أمر له أهمية بالغة في تفعيل نشاط الصيرفة الالكترونية ، فمن خلال الأمن المعلوماتي فإن الخدمة المصرفية سوف تتمتع بجميع خصائص جودتها وعلى رأسها السرية والخصوصية والموثوقية والمتاحية التي توفر خدمة مصرفية بكافة المقاييس ،كل هذا من شأنه أن يزيد من ثقة الزبون بالخدمات المصرفية الالكترونية لظروف الراحة والأمان التي يشعر بها، ومن هنا نستنتج أن الأمن المعلوماتي لا يلعب دورا فقط في جودة الخدمات المصرفية الالكترونية ولكنه هو أساس وجودة الخدمة المصرفية.

اختبار الفرضيات : من خلال مسار الدراسة تم التأكد من صحة الفرضية المطروحة في بداية الدراسة والقائلة بأن جودة منتجات الصيرفة الالكترونية تتوقف على فاعلية الأنظمة المعلوماتية التي تضمن سرية الخدمة وإتاحتها في الوقت المناسب لطالبيها حيث أكدت الدراسة بأن الأمن المعلوماتي هو الشرط الأساسي لتمتع الخدمة المصرفية الالكترونية بخصائصها ومتطلباتها لاسيما تلك المتعلقة بالسرية والتي تعتبر شرط أساسي لعامل الثقة الذي يعزز من ولاء الزبائن لمصارفهم .

النتائج : من خلال الدراسة توصلنا إلى النتائج التالية:

– الصيرفة الالكترونية تعني التسليم التلقائي لمنتجات وخدمات المصارف الحديثة والتقليدية إلى يد العميل أو المستثمر بصورة مباشرة عبر الطريق الالكتروني وقنوات الاتصال التفاعلية.

– الأمن المعلوماتي هو الحقل الذي يدرس طرق حماية البيانات المخزنة في أجهزة الحاسوب إضافة إلى الأجهزة الملحقة و شبكات الاتصالات و التصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزنة أو تلك التي ترمي إلى نقل أو تغيير أو تخريب القواعد المعلوماتية .

– يتم على مستوى المصرف بناء إستراتيجية شاملة لأمن المعلومات تتناول نظام المصرف وموقعه الافتراضي وتتناول نظم الحماية الداخلية من أنشطة إساءة الاستخدام التي قد يمارسها الموظفون المعنيون داخل المنشأة وتحديدا الجهات المعنية بالوصول إلى نظم التحكم والمعالجة والمبرمجين ، إستراتيجية الحماية من الاختراقات الداخلية ، هذه الاستراتيجيات يجب أن تمتد إلى عميل المصرف لا للبنك وحده ، حتى نضمن نشاطا واعيا للتعامل مع المعلومات وتقدير أهمية حمايتها ، ولكل إستراتيجية أركانها ومتطلباتها ومخرجاتها ، وتقييم كفاءة الإستراتيجية يقوم على مدى قدرتها على توفير مظلة امن شاملة لنظام المصرف والعميل والنظم المرتبطة بهما.

– من ضمن عوائق الصيرفة الالكترونية هو غياب النصوص القانونية التي تقوم بردع الجرائم الالكترونية.

التوصيات: بناء نتائج الدراسة نقدم التوصيات التالية:

- ضرورة تركيب برنامج مضاد للفيروسات ملائم لنظام التشغيل المستخدم في جهاز الحاسوب و يجب أن يكون نسخة أصلية للاستفادة من الدعم الفني للشركات التي يتم شراء البرامج المضادة منها .
- ضرورة إتخاذ الإجراءات الإحترازية لحماية الموقع و تحصينه من أي تخريب أو سطو و حمايته من الأخطار بما فيها الأخطار الطبيعية والعمل على إدامة مصدر القدرة الكهربائية و انتظامها و تحديد أساليب و إجراءات التفتيش و التحقق من هوية الأفراد الداخلين و الخارجين من الموقع و عمل سجل لذلك.
- توعية عملاء البنوك بعمليات الاحتيال والنصب المالي والمصرفي الإلكتروني وبعمليات الاحتيال التي تتعرض لها البطاقات المصرفية أو البطاقات الائتمانية.
- تحديد مواصفات محددة للعاملين و وضع تعليمات واضحة لاختيارهم و ذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد إضافة إلى وضع الخطط لزيادة الحس الأمني و الحصانة من التخريب.
- المراجعة الدورية للتدقيق في شخصية وسلوك الأفراد العاملين من وقت لآخر و ربما يتم تغيير مواقع عملهم و محاولة عدم احتكار المهام على موظفين محدودين .
- ضرورة قيام الدولة بوضع قوانين وتشريعات شاملة فيها يخص التعامل بشبكة الويب، وتحمل عقوبات مخصصة لجرائم الانترنت خصوصا المتعلقة بالعمل المصرفي.

- ضرورة قيام الدولة بوضع قوانين وتشريعات شاملة تحكم التعامل بالصيرفة الالكترونية، تحدد فيها مسؤوليات وواجبات كل من المصرف والعميل.

قائمة المراجع :

[i] شيرين بدري البارودي، **دور اقتصاد المعرفة في تطوير الخدمات الالكترونية (دراسة تحليلية عن البنوك الالكترونية)**، المؤتمر العلمي الخامس " اقتصاد المعرفة والتنمية الاقتصادية"، جامعة الزيتونة، الأردن، 2005، ص07.

[ii] المرجع السابق، ص08.

[iii] هشام عبد القادر، **البنوك الالكترونية** ، (بحث غير منشور)، جامعة القاهرة، مصر، 2013، ص02.

[iv] آيت عكاش سمير، سعيد لهواري، **البنوك الالكترونية وعمليات غسيل الأموال**، الملتقى العلمي الدولي الخامس حول "الاقتصاد الافتراضي وانعكاساته على الاقتصاديات الدولية"، المركز الجامعي خميس مليانة، الجزائر، 2012،ص06.

[v] يوسف مسعداوي، **البنوك الالكترونية** ، ملتقى المنظومة المصرفية الجزائرية والتحولات الاقتصادية–واقع وتحديات–، جامعة الشلف –الجزائر، 2004، ص232.

[vi] هشام عبد القادر ، مرجع سابق ، ص 13.

[vii] يوسف مسعداوي ، مرجع سابق ، ص 233.

[viii] نفس المرجع السابق 233.

[ix] منصور بن سعيد القحطاني ، **مهددات الأمن المعلوماتي وسبل مواجهته ا**، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2008م، ص33

[x] عائض المري، **أمن المعلومات ماهيتها وعناصرها وإستراتيجيتها**، (بحث غير منشور)، الكويت، 2013، ص01.

[xi] منصور بن سعيد القحطاني، مرجع سابق، ص47.

[xii] سلمان بن علي بن وهف القحطاني، **أمن المعلومات في ضوء التقني والتكنولوجي الحديث في الشبكات اللاسلكية النقالة**، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي – مركز البحوث والدراسات،: دبي ، الأمارات العربية المتحدة، 2003، ص 10.

[xiii] عطا الله أحمد الحسبان، **مدى تعامل مدققي أنظمة تكنولوجيا المعلومات بمعايير التدقيق الدولية الخاصة ببيئة أنظمة المعلومات للمحافظة على امن وسرية المعلومات في البنوك التجارية الأردنية** ، جامعة اربد الأهلية ، الأردن ، 2012 ، ص 362 .

[xiv] هشام عبد القادر،مرجع سابق، ص13.

[xv] سلمان بن علي بن وهف القحطاني، مرجع سابق، ص 11.

[xvi] معين ثابت عارف، **الصيرفة الالكترونية: خدمة مالية تجاوزت الزمان والمكان**، (بحث غير منشور)، الجامعة المستنصرية للدراسات العليا، بغداد، العراق، 2012.