Lerner, M. La protection d'information dans le systeme de paiements bancaires electroniques [Text] / M. Lerner, R. Pavlov, S. Smirnov // Міжнародна банківська конкуренція: теорія і практика : рбірник тез доповідей V Міжнародної науково-практичної конференції (27 -28 травня 2010 р.) : у 2 т./ Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України».– Суми, 2010. - Т. 2. - С. 103-104.

M. Lerner, R. Pavlov, *c.s.e. chargé de cours,* ***S. Smirnov,*** *d.s.f-m. prof.,*
Université nationale de Dnipropetrovsk Oles Gontchar

LA PROTECTION D'INFORMATION DANS LE SYSTEME DE PAIEMENTS BANCAIRES ELECTRONIQUES

Les systèmes des paiements électroniques sont apparus relativement récemment sur le marché des services bancaires de l'Ukraine. Un système "Client-Banque" avait aparu au début des années 90. C'est l'ensemble des éléments techniques et logistiques destinés à la conduite rapide par le client des ses comptes à la banque, et ainsi pour l'échange des documents de paiement et l'information correspondante technologique entre la banque et ses clients sous la forme électronique. Il y a un réseau original informatique à l'utilisation de ce système, qui unit les parties de client et bancaires du système "Client-Banque". L'échange d'information dans un tel réseau permet au client de réaliser le contrôle des ses comptes bancaires, effectuer les paiements, recevoir les relevés etc. Bien que le système "Client-Banque" assure le mouvement seulement d'un petit cercle des opérations de comptes – le mouvement des documents de comptes – déjà aujourd'hui en Ukraine, même à l'utilisation du système seulement par un tiers de clients, "Client-Banque" fait le mouvement des moyens dans les terminaux près de 70 % du chiffre d'affaires total des moyens dans le système bancaire. En conséquence aujourd'hui l'attention spéciale est portée à l'introduction des systèmes "Client-Banque" à la base des technologies modernes. Le logiciel établi aux banques JOB, qui permet de traquer l'entrée par virement des moyens pour les comptes des clients en régime du temps réel et effectuer les paiements des clients en tenant compte de ces entrées.

La plus importante tâche, qui faisait face aux concepteurs du système "Client-Banque", était la protection de l'information, qui est transmise en forme du jeu de données dans le Réseau-Internet. On utilisait pour cela l'algorithme RSA qui est un premier algorithme cryptographique avec la clé ouverte, utile pour chiffrer des données et pour SED. Puisque SED assure autentification de l'auteur du document et la confirmation de l'intégrité du contenu, elle sert de l'analogue de la signature à la main à la fin du document. Un des échangeurs par les messages après le contrôle de la réalité de la signature digital peut transmettre le message signé encore à quelqu'un, qui pourra contrôler aussi cette signature.

Pour chiffrer et déchiffrer des données transmises on utilise le système des clés formant la paire. Elle consiste en ce que le message du client est chiffré avec l'aide de la clé confidentielle du client et la clé ouverte de la banque. Ainsi, ces données peuvent être déchiffrées seulement avec l'aide de la clé confidentielle de la banque et la clé ouverte notamment du client. À la demande de NBU le client utilise deux clés de la signature électronique, qui s'appellent "la clé du directeur" et "la clé du comptable". D'abord le document est signé par "la clé du comptable", s'impose ensuite SEC "la clé du directeur". Ainsi, le document a double cryptografie. Ensuite, pendant l'expédition du document à la banque, il est chiffré

en supplément par “la clé de transport”. Ainsi, le document est protégé par trois SEC dans le canal de la transmission des données.

Le serveur bancaire du système “Client-Banque” est physiquement séparé du serveur de la base des données JOB. La banque utilise la technologie suivante du traitement du document de client: le serveur “Client-Banque” contrôle la signature de “la clé de transport” sur le document et le retire; se photographient plus loin alternativement les signatures du “directeur” et “du comptable”. Le serveur JOB, à son tour, contrôle la convenance du remplissage des espaces informatiques du document et, en l’absence des erreurs, l’insère dans la base de données JOB avec la préservation de l’information en ce qui concerne les signatures du “comptable” et “du directeur”. Ainsi, l’opérateur de la banque a la possibilité de contrôler la conformité SED au document et au client, c’est à dire, l’origine du document. En effet, le système est assez sûr et protégé contre l’intervention non sanctionnée.