СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРБЕЗПЕКИ БАНКІВСЬКИХ РАХУНКІВ ТА БАНКІВСЬКИХ БУДІВЕЛЬ

асистент Булага В.А., студент Передерій І.А.
Харківський національний університет радіоелектроніки,
комп'ютерної радіоінженерії та систем технічного захисту інформації,
м. Харків, Україна
e-mail: victoria.bulaga@nure.ua, illia.perederii@nure.ua

Abstract. This work is dedicated to the importance of financial security of the banking system of Ukraine and conducting a comprehensive assessment of the current situation. An analysis of the protection and insecurity of the current bank was carried out. The technical details of the bank's security system have been reviewed. Cybersecurity of banking and banking sectors is an important part of our economy. However, cyber-attacks are becoming increasingly sophisticated, and banks are at risk of losing their efforts to protect the data of their clients. By keeping up to date with the latest security technologies and best practices, banks can continue to provide their clients with safe and reliable banking services.

Ключові слова: банківська безпека, кібербезпека , брандмауери, шифрування.

Вступ. Сьогодні кожна людина має свою банківський рахунок у банку, їх безпека є дуже важливою економічним аспектом у розвитку України та взагалі будь-якого континенту. Безпека країни складається з безпеки її структурних і насамперед із безпеки її первинної ланки господарювання [1, 2]. Про це свідчить реакція впливу ринкової конкуренції на економіку країни в цілому та економіку окремого підприємства або банка. Для соціально орієнтованої економіки країни конкуренція є двигуном її розвитку та вдосконалення, і в інтересах держави захистити її всіма можливими засобами. Таким чином, банківська безпека з одного банку є складовою частиною системи національної безпеки, поряд з такими її елементами як технічна безпека, енергетична, військова, екологічна, інформаційна та інше. При цьому слід враховувати, що однією з найбільш небезпечних загроз для економіки України є порушення її фінансово-банківської системи. На сьогодні склалася така ситуація що крадії все більше і більше намагаються хакнути наші картки та забрати ваші гроші, тому мета цього реферату розповісти про те як банківська система захищає ваші збереження так, та що робити якщо ви загубили вашу карту, і як не втратити всі ваші гроші [3, 4].

Банківська система України сьогодні переживає важкі часи, реагуючи, як лакмус, на зміни як в економічному, так і соціально-політичному середовищі країни. Соціально-політична криза в Україні 2013-2014 рр. спричинила глибоку економічну кризу, яка найбільше вплинула на

банківську сферу. До систем безпеки банків завжди пред'являлися підвищені вимоги, і уявити собі банк без охоронної та тривожної сигналізації, системи контролю доступу та відеоспостереження неможливо. Щоб отримати дозвіл на відкриття офісу банку, додаткового офісу та відділення потрібно здати систему безпеки спеціальної комісії. Засоби забезпечення безпеки охоплюють організаційні заходи, інформаційне забезпечення, нормативно-методичні матеріали, роботу з персоналом, засоби фізичної захисту, засоби протидії тощо.

Система контролю доступу до банку. Основне призначення СКД у банку - запобігання проникненню небажаних осіб у приміщення, що охороняються банку. Мережева система контролю доступу до банку повинна працювати під управлінням центрального сервера системи у межах відділення. Бажано, щоб СКД усіх філій та додаткових офісів банку працювали в рамках єдиної системи з адмініструванням та контролем з центрального офісу.

Відео контроль у помешканні та прилеглій території банку. Ситуаційне відеоспостереження для банку – основний інструмент оперативного контролю служби безпеки. При оснащенні банку системами відеоспостереження сповідається принцип тотального контролю всієї території. Виняток становлять лише кабінети в офісній частині банку. Відеокамери контролюють: операційний зал, зону самообслуговування, банкомати та терміналі, касовий вузол і кабіни кас, комора і шляхи проходження грошових коштів, зону інкасації, внутрішній двір і периметр. Сучасні технології дозволяють отримувати зображення високої якості, що дуже важливо для проведення розслідувань та передачі матеріалів до правоохоронних органів. Дозвіл IP-камер і HD-SDI досягає FullHD і більше, а швидкість до 60 к/с. Від такої камери неможливо сховатися. Шкірна деталь того, що сталося буде зафіксована у найдрібніших подробицях.

Відеоспостереження у банку для контролю за обслуговуванням клієнтів та завдань маркетингу. Системи відео аналізу сьогодні пропонують широкий набір інструментів, що допомагають підвищити ефективність та контроль роботи банківського відділення: 1) підрахунок відвідувачів; 2) підрахунок довжини черги.

Програмні та апаратні засоби захисту інформації. Усі платіжні документи СЕП перед відправленням з банку обробляються апаратно-програмними засобами захисту інформації, що забезпечують виконання таких вимог з точки зору безпеки інформації: інформація, що передається, має бути закритою, тобто повідомлення може бути прочитане лише тим, кому воно адресоване; цілісність — випадкове чи навмисне пошкодження повідомлення на етапі його передачі буде виявлене під час його прийому; автентичність відправника (під час прийому повідомлення можна однозначно визначити, хто його відправив).

Низка допоміжних вимог, що дає змогу більш детально аналізувати можливі нестандартні ситуації: 1. Засобами захисту інформації ведеться шифрований арбітражний журнал, в якому зберігається протокол обробки інформації, а також вміст файлів, що обробляються; 2. У шифроване повідомлення включені поля дати та часу обробки.

Основними засобами захисту інформації в СЕП є апаратні засоби. Секретність ключів у них забезпечується технологічно: 1. Ключі зберігаються в спеціальній електронній картці, прочитати їх можна тільки за допомогою спеціального блоку, що виконує процес шифрування інформації. Прочитати ключі іншими засобами неможливо; 2. Електронна картка видається банку з попередньою прив'язкою її до конкретного блоку шифрування цього ж банку; втрачена чи викрадена картка не буде працювати в іншому шифро-блоці (наприклад, в апаратурі іншого банку); 3. У випадку крадіжки одночасно блоку і картки у конкретного банку передбачено режим виключення цієї апаратури зі списку користувачів СЕП; банк може продовжити роботу в СЕП після вирішення юридичних та фінансових питань, пов'язаних з втратою апаратури та отриманням нового комплексу. Найбільш слабким місцем з точки зору безпеки є ділянка підготовки платежів персоналом банку - учасника СЕП. Всі зареєстровані більш-менш успішні спроби НДС були з боку представників банків, що призводило до крадіжки коштів у власного банку, а не в держави чи в інших банках. В усіх цих випадках особи, які робили спроби НДС, мали легальний доступ до системи підготовки та захисту платіжної інформації, причому їх повноваження були перевищені (доступ до багатьох чи навіть до всіх банківських ресурсів системи).

З метою гарантування безпеки інформації на цій ділянці від учасників СЕП вимагається виконання низки організаційних вимог: 1. Допуск тільки довірених осіб до ключових операцій підготовки платіжних документів; 2. Виконання відповідальними особами банку постійного, реального та достатнього контролю за станом бухгалтерського балансу та кореспондентського рахунку банку. Всі повноваження щодо доступу до програмно-апаратних засобів банку недоцільно зосереджувати в особі одного співробітника банку: за кожну ділянку обробки платежів має відповідати окремо уповноважений (адміністратор локальної мережі, адміністратор електронної пошти, відповідальний за роботу АРМ-3 СЕП і т. ін.). Для гарантування безпеки інформації на рівні банків—учасників СЕП пропонується впровадження перехресного накладення електронного підпису на платіжні документи. Банкам пропонується використання програмних засобів, що реалізують цифровий підпис, реалізований на основі алгоритму RSA. Кожний учасник обміну електронними документами має два ключі: 1.Секретний, що повинен ретельно оберігатися від сторонніх осіб і бути відомим тільки його власнику;

2.Відкритий, що розповсюджений в системі і може бути відомим кожному учаснику системи.

Суть алгоритму RSA. 1. В основу електронного цифрового підпису покладено оброблене спеціальним секретним ключем відправника і відкритого ключа отримувача повідомлення.

2. Під час перевірки електронного цифрового підпису програмним комплексом отримувача формується прототип електронного підпису отриманого повідомлення.

3. Отриманий цифровий підпис дешифрується відкритим ключем відправника і секретним ключем отримувача повідомлення і вираховується прототип електронного цифрового підпису.

4. Отриманий прототип порівнюється з обрахованим прототипом електронного цифрового підпису. Збіг цих двох прототипів підпису (отриманого та обчисленого) показує, що повідомлення було підписане зазначеним відправником інформації та отримане у тому ж вигляді, в якому воно було підписане.

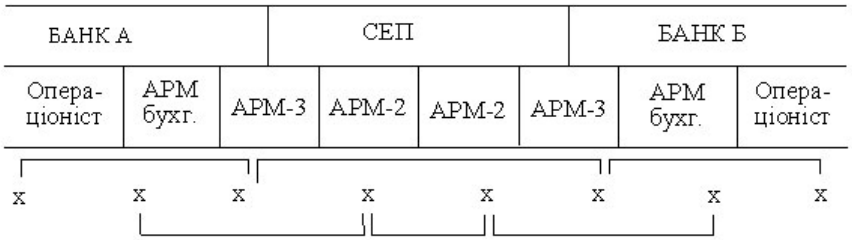

Рисунок 1 – Схема накладення електронного цифрового підпису в СЕП

Висновки. Кібербезпека банківських рахунків та банківських будівель є дуже важливою частиною нашої економіки . Вона є головним пріоритетом для банків, оскільки вони обробляють конфіденційну фінансову інформацію та транзакції. Залишаючись у курсі найновіших технологій безпеки та найкращих практик, банки можуть продовжувати забезпечувати своїм клієнтам безпечні та надійні банківські послуги.

Список використаних джерел.

1. Сердюк С. Л. Цифрова система для митного контролю ручного багажу в аеропортах та зонах підвищеної небезпеки / С. Л. Сердюк, В. А. Булага // Радіоелектроніка та молодь в XXI столітті : матеріали 26-го Міжнародного молодіжного форуму, 24-25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – Т. 3. – С. 132–133.

2. V. Bulaga. Digital System for Customs Inspection of Baggage in High Security Areas // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 43-46. DOI: 10.35598/mcfpga.2021.015

3. https://rating.zone/chem-obernetsia-dlia-ukrayny-rekordnyj-rost-tsen-na-syrevye-tovary/

4. https://osvita.ua/vnz/reports/bank/20375/