

УДК 004.056

Зайко Т.А.¹, Дем'янова Д.К.²

¹канд. техн. наук, доц. НУ «Запорізька політехніка»

²студ. гр. КНТ-128 НУ «Запорізька політехніка»

КІБЕРБЕЗПЕКА, КІБЕРЗАХИСТ ТА ІНФОРМАЦІЙНА БЕЗПЕКА БАНКІВСЬКОЇ СФЕРИ В УКРАЇНІ

Сучасна банківська система значно залежить від надійності інформаційних технологій, які вона використовує. Тому кібербезпека і кіберзахист стали фундаментальними засадами існування банківської системи взагалі. Стрімка інформатизація та розвиток глобальних інформаційно-комунікаційних мереж окрім автоматизації звичних банківських процесів ще й постійно надають можливості створення нових банківських продуктів (послуг) (сьогодні це «SMS-банкінг», «Інтернет-банкінг», «WebMoney Banking» тощо).

Найбільш суттєвими загрозами безпеці інформаційних ресурсів є витік або втрата ресурсів (зокрема відомостей, що становлять банківську таємницю). Загрози інформаційним ресурсам можуть бути реалізовані шляхом підкupu осіб, необережного, недбалого поводження з банківською таємницею, недотримання вимог збереження інформації з обмеженим доступом.

Задля збереження інформаційної безпеки банківської системи телекомунікаційне середовище повинно за вимогами ISO (Міжнародна організація стандартизації) забезпечити:

- захист інформації при її зберіганні, обробці та передачі по мережах;
- підтвердження справжності даних і користувачів;
- виявлення та попередження порушення цілісності даних;
- захист програмних продуктів від впровадження програмних закладок і «вірусів»;
- захист від несанкціонованого доступу до інформаційних ресурсів тощо.

У зв'язку з цим банк використовують системи передачі повідомлень та здійснення міжбанківських операцій, як один із методів захисту інформації.

Наприклад, у США використовуються Fedwire – мережа федеральної резервної банківської системи, CHIPS – міжбанківська платіжна мережа, Bankwire. У Франції міжбанківські розрахунки засновані на системі SIT. У Великобританії застосовуються системи CHAPS (Clearing Houses Payment System) і BACS (Bankers Automated Clearing Services).

Спеціальна мережа передачі банківських повідомлень на міжнародному рівні S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunications) – одна з найбільших у світі систем банківських повідомлень. Вона створена задля забезпечення всім учасникам доступу до цілодобової високошвидкісної мережі передачі банківської інформації в стандартній формі за високого ступеня контролю і захисту від несанкціонованого доступу. У цілому система SWIFT являє собою глобальну всесвітню мережу на основі комп'ютерних центрів, з'єднаних різними каналами зв'язку.

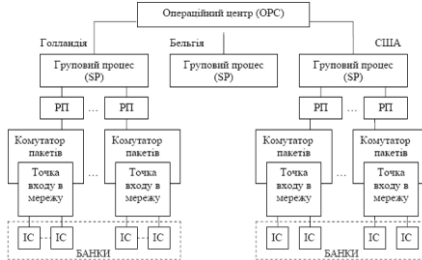


Рисунок 1 – Архітектура SWIFT

Усі питання, пов'язані з безпекою в системі S.W.I.F.T., умовно можна поділити на такі розділи:

- фізична безпека;
- безпека логічного доступу до системи S.W.I.F.T.;
- забезпечення безпеки повідомлень, переданих і збережених у системі;
- безпека обміну повідомленнями “користувач – користувач”.

Говорячи про програмно-апаратну реалізацію системи SWIFT, слід зазначити той факт, що всі можливі варіанти такої реалізації теж чітко стандартизовані. Як інтерфейси різних рівнів для підключення до мережі SWIFT використовуються інтерфейси ST200, ST400 і ST500, які мають різну продуктивність і можуть бути реалізовані на основі різних комп'ютерних платформ.

Банківська сфера з часом вдосконалює методи захисту інформації, такі як системи передачі повідомлень та здійснення міжбанківських операцій. Існує декілька платіжних мереж по всьому світу, але найпоширенішою наразі

є система SWIFT, до якої підключено багато українських банків. Вона має чіткі вимоги до безпеки, які базуються на міжнародних стандартах.