Годован В.В., магістр,
Ставська В.С., студентка,
Житомирський державний технологічний університет

ШЛЯХИ УДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ БАНКОМАТІВ

Сьогодні спостерігається інтенсивний ріст та розвиток банківських послуг та систем самообслуговування (банкоматів, платіжних терміналів). Як стверджують спеціалісти по банківським технологіям, зараз у всьому світі функціонує приблизно 1,4 млн. банкоматів різних типів. Сучасні банкомати стають все більш інтелектуальними та функціональними. Якщо перші моделі тільки вміли працювати з магнітною полосою кредитних карт, то сучасні машини можуть обробляти «чіпові карти», а також виконувати велику множину функцій. Сьогодні користувачі можуть здійснити за допомогою банкомату різноманітні платежі: поповнювати рахунок мобільного оператору зв'язку, сплачувати комунальні платежі і т.п.

Однак для реалізації всіх цих можливостей необхідна надійна інформаційно-комунікаційна мережа, що відповідає за передачу даних.

У світі вже зафіксовано цілий ряд інцидентів, коли великі мережі банкоматів під управлінням Windows виходили зі строю, дякуючи комп'ютерним вірусам. У всіх випадках банкомати виявлялися відключеними від загальної інформаційно-комунікаційної мережі на декілька годин.

Таким чином мережі банкоматів можуть бути схильні до наступних видів загроз: вірусні атаки, зловмисні дії персоналу, помилки адміністратора та ін. Крім цього часто банкомати зосереджуються в неконтрольованих зонах, здійснюючи зв'язок з банком через публічні мережі.

На рисунку 1 показано проект модернізованої інформаційно-комунікаційної мережі. Умовні позначення: R_Centr – центральний маршрутизатор (hub), що розташований у Центральному офісі; R_X – маршрутизатори, що розташовані у регіональних відділеннях банку, X – номер внутрішньої мережі регіонального відділення; SW_X – комутатори, X – номер комутатора; WS_X_Y – робочі станції операторів, X – номер внутрішньої мережі, Y – номер робочої станції.

При побудові модернізованої мережі за основу було взято загальну інформаційно-комунікаційну мережу XXX банку в Україні. Перед безпосереднім налагодження захищеної ІКМ, було здійснено проектування схеми мережі в середовищі-емуляторі GNS.

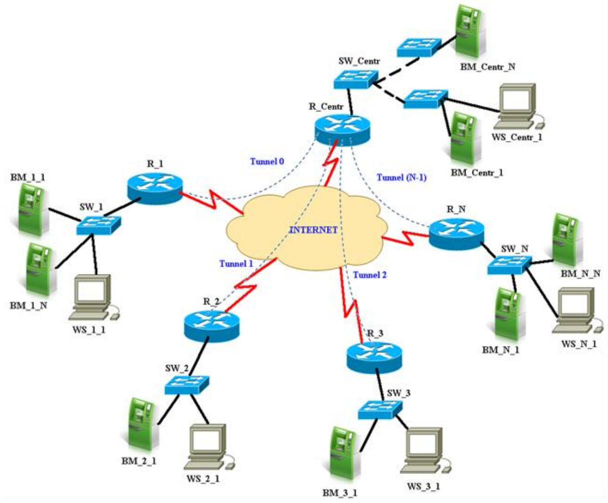

Рис1. Проект захищеної ІКМ

Проведена розробка та тестування програми функціонування підсистеми інженерно-технічного захисту банкоматів комерційного банку суттю якої є управління системою охорони банкоматів від несанкціонованого доступу на базі контролера MaxyConFlexy за допомогою спеціального програмного середовища в емуляторі роботи контролера «Конфігуратор FBD». Головне вікно програми, що відображається на екрані контролера представлене на рис.2

Рис.2. Вигляд головного вікна програми

За допомогою розробленої програми роботи контролер здійснює контроль за сигналами датчиків та проводить ввімкнення сирени при виявленні сигналу тривоги.