УДК 003.26.09

МЕТОДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Великий Владислав, Мороз Юрій, Полотай Орест

кафедра безпеки інформаційних технологій Національного університету «Львівська політехніка»,
кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

В даній роботі проведено детальне ознайомлення із технічним захистом інформації, а також розглянуто апаратний модуль безпеки (HSM) для зберігання, керування, генерування та використання ключів шифрування.

***Ключові слова**: технічний захист інформації, криптографічний захист інформації.*

In this paper, a detailed acquaintance with the technical protection of information, as well as a hardware security module (HSM) for storage, management, generation and use of encryption keys.

***Key words:** technical protection of information, cryptographic protection of information.*

Сучасний світ важко уявити без використання інформаційно-комунікаційних систем, які б не опрацьовували чутливу інформацію, наприклад дані медичних карток, інформацію про банківські рахунки та інші види особистої інформації. Тому питання інформаційної безпеки, відіграє значну роль у життєдіяльності кожного. З іншого боку роль інформаційної безпеки дуже сильно недооцінена. Багато хто розуміє її важливість, але в більшості випадків дії обмежуються встановленням базового мережевого екрану на кордоні мережі та/або звичайних антивірусних програм. В інших випадках кожен сподівається на те, що напад станеться з кимось іншим.

Зі збільшенням диджіталізації набирали обертів і зловмисники, метою яких було отримання персональних даних. Саме тому, гостро постало питання технічного захисту інформації.

Розвиток сучасних та високоефективних методів шифрування та криптографії зіграло ключову позицію в захисті інформації. Сьогодні практично будь-яка комунікація в мережах виконується із застосуванням криптографічних систем шифрування інформації та комбінації даних систем. Однією із проблем є те, що чутлива інформація зберігається на носіях даних разом із ключами, які використовувались для шифрування цієї інформації. Зловмисники, які отримували доступ до носіїв чутливої інформації могли з легкістю отримати доступ до ключів, які використовувались для криптографічного захисту даних, що давало їм змогу без перешкод отримати чутливу інформацію. Ще однією проблемою було те, що потрібно було постійно передавати ключі по мережі, що становило загрозу перехоплення ключів методом сніфінгу. Сніфінг – процес перехоплення і аналізу мережевого трафіку. Після чого постало питання безпечного зберігання, використання ключів шифрування та захист від витоку ключів під час віддаленого злому систем.

Мета даної роботи – розглянути сучасні методи технічного захисту цінних ключів, ознайомитися із апаратними засобами для зберігання, керування, генерування ключів і обробки інформації з використанням даних ключів на прикладі апаратного модуля безпеки.

Актуальними проблемами даної теми є:

- наразі, застосування сучасних технічних засобів захисту інформації не набуло великого поширення;
- технічні засоби захисту інформації є складними у використанні;
- практично відсутня конкуренція на ринку технічних пристроїв даного типу;

- обмеження продуктивність традиційних HSM
- в більшості випадків технічні пристрої є дороговартісними.

Розроблений підхід з використанням HSM (Hardware Security Module) пропонує взагалі не давати вразливій частині системи доступ до вмісту ключа. HSM – це фізичний пристрій, підключається напряму до хоста або сервера, який зберігає чутливу інформацію.

В такому випадку перед апаратним модулем безпеки ставляться наступні завдання:

- зберігання, керування, генерування цифрових ключів або іншої секретної інформації;
- виконання криптографічних операцій з допомогою секретних ключів;
- виконання криптографічних операцій не повинно відбуватись за межами апаратного модуля безпеки, а користувач має повинен отримувати доступ тільки до результатів операцій.

Результати проведеного аналізу говорять про те, що даний продукт буде корисним для використання банківськими установами, медичними закладами, компаніями, які зберігають і обробляють дані банківських карток та персональні дані користувачів.

Література:

1. https://hubsecurity.io/what-is-a-hardware-security-module-hsm/
2. https://habr.com/ru/company/JetBrains-education/blog/251243/
3. https://www.advantio.com/blog/hardware-security-module-hsm-what-is-it-and-what-is-its-role-in-protecting-payment-card-data