НАЦІОНАЛЬНА БЕЗПЕКА

Махітько В.С., Полійчук М.В.
студентки,
Науковий керівник: ***Беркут О.В.***
старший викладач,
Університет митної справи та фінансів

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКИХ СТРУКТУРАХ

В останні роки в Україні реалізовано ряд практичних заходів стосовно підвищення рівня банківської безпеки. Як результат сформована система нормативно-правового та організаційного забезпечення інформаційної безпеки банків, реалізовано практичні заходи по удосконаленню засобів інформаційної безпеки в таких структурах. Разом із тим, рівень інформаційної безпеки банків на сьогоднішній день не відповідає об'єктивним вимогам, і стан захисту від злочинних посягань залишає бажати кращого [1, с. 187].

Більшість систем захисту банківських даних реалізується на основі криптографічних методів перетворення інформації. Під криптографічним захистом інформації розуміється таке перетворення вихідної інформації, в результаті якого вона стає недоступною для ознайомлення та використання особами, які не мають на це повноважень.

Відомі різні підходи до класифікації методів криптографічного перетворення інформації. За видами впливу на вихідну інформацію ці методи можуть бути розділені на чотири групи (рисунок 1).

Прикладом програмної реалізації захисту банківських даних є програмні засоби криптографічного захисту інформації «Грифон-Б» та «Грифон-Л» призначені для криптографічного захисту конфіденційної інформації в автоматизованих банківських системах та застосовуються для обміну інформацією всередині корпоративної мережі банку, з клієнтами, що працюють з системою «Клієнт-Банк», в системах обслуговування пластикових карток.

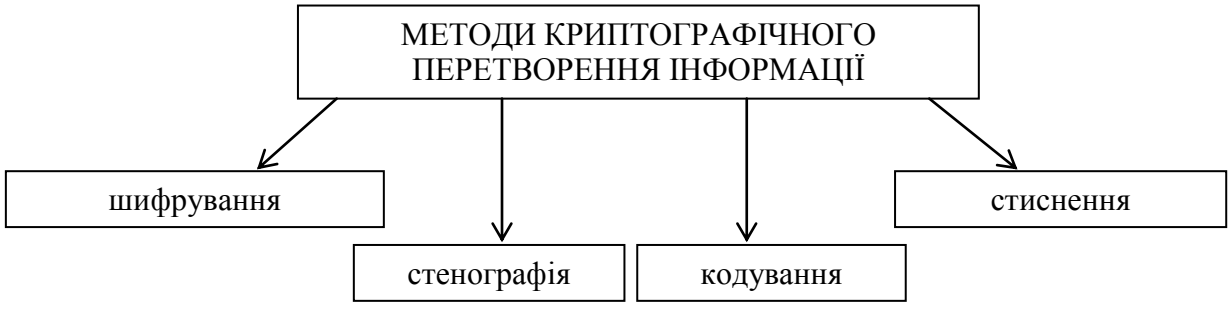

Рис. 1. Методи криптографічного перетворення інформації

Джерело: розроблено авторами

Бібліотека процедур криптографічного захисту інформації «Тайфун-PKCS#11» містить процедури, призначені для забезпечення захисту цілісності й конфіденційності інформації, виконання автентифікації відправників повідомлень із використанням механізмів криптографічного захисту (електронний цифровий підпис, шифрування, вироблення імітовставок і геш-функцій) шляхом вбудовування в конкретні прикладні системи [2, с. 92].

Якщо розглядати захист персональних даних з боку застосування програмно-технічних засобів захисту, то тут можна виділити спеціалізовані системи моніторингу подій інформаційної безпеки.

Одним із прикладів подібних систем є продукт ArcSight ESM. ArcSight ESM – це провідна платформа на ринку для моніторингу корпоративних загроз і ризиків безпеки, яка займає одну з лідируючих позицій в даній області [3, с. 34].

Цей продукт стане в нагоді:

1) службі інформаційного контролю та аудиту (коли необхідно отримати задовільну оцінку аудиту);

2) службі інформаційної безпеки (коли необхідно визначити хто хоче отримати доступ до інформації, і чи є у цієї особи відповідні повноваження);

3) службі IT (коли інфраструктура повинна відповідати вимогам затвердженої політики і ми повинні швидко реагувати на нові загрози).

На сьогодні відома ще одна цікава послуга в галузі захисту інформації – тест на проникнення. Це практичний спосіб показати, наскільки захищена компанія від зазіхань на її конфіденційні дані та інших загроз для інформації. За кордоном часто зустрічається термін етичний хакінг. Даний метод симулює набір «хакерських» атак, цілі яких – проникнення у внутрішню інфраструктуру мережі компанії, крадіжка та модифікація конфіденційних даних, порушення роботи критичних бізнес процесів компанії. Кожен банк може перевірити свою систему безпеки на надійність і, виходячи з результатів цієї перевірки, вживати необхідних заходів. Ця послуга являє собою імітацію послідовності дій зломщика щодо здійснення несанкціонованого проникнення в інформаційну систему замовника [3, с. 35].

Отже, забезпечення інформаційної безпеки банку – це складна система заходів із забезпечення необхідного рівня інформованості керівництва і персоналу банку, а також зовнішнього середовища, ефективний захист усіх видів інформації від зовнішніх і внутрішніх загроз, що досягається організацією збору інформації про внутрішнє і зовнішнє середовище банку, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів та конкурентів; дотриманням відповідних режимів діяльності банку; виконанням усіма працівниками банку норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів витоку інформації та їх нейтралізації.

Таким чином необхідно використовувати криптографічні алгоритми шифрування, що стандартизовані й сертифіковані Національним банком України. Поява національних стандартів за спеціальними механізмами забезпечення інформаційної безпеки банків (шифрування, цілісність даних,

автентифікація) може суттєво вплинути на рівень забезпечення інформаційної безпеки банківських транзакцій і надійності банківської системи взагалі.

Список використаних джерел:

1. Колодій І. М. Принципи та методи захисту банківської інформації / І. М. Колодій // Університетські наукові записки. – 2010. – № 2. – С. 186-191.

2. Король О. Г. Аналіз загроз і механізмів забезпечення безпеки інформації в системі електронних платежів комерційного банку України / О. Г. Король // Системи обробки інформації. – 2015. – № 9 (134). – С. 88-95.

3. Курченко О. А. Підвищення ефективності системи управління захистом персональних даних клієнтів банку / О. А. Курченко // Сучасний захист інформації. – 2014. – № 1. – С. 32-37.

Покровська А.В.

аспірант,
Національний інститут стратегічних досліджень
при Президентові України

НИЗЬКОТЕХНОЛОГІЧНИЙ ТЕРОРИЗМ ЯК КЛЮЧОВА ЗАГРОЗА В ЕПОХУ ВИСОКИХ ТЕХНОЛОГІЙ

Тероризм як асиметричний метод досягнення політичних, ідеологічних, релігійних чи інших цілей насильницьким шляхом не стоїть на місці та змінюється разом із трансформаціями у середовищі, де він застосовується. Із розвитком новітніх, зокрема інформаційних, технологій терористи отримали широкі можливості для поширення своєї ідеології, пошуку новобранців, координації терористичних мереж на різних рівнях та контролю за виконанням терористичних актів. Після подій 11 вересня та внаслідок розповсюдження США дискурсу глобальної війни з тероризмом закономірним стало побоювання того, що терористи надалі намагатимуться вчиняти ще більш масштабні теракти, не полишатимуть спроб отримати доступ до зброї масового ураження та користуватимуться передовими досягненнями людства для реалізації злочинних намірів. Однак досвід останнього десятиліття свідчить про те, що терористи надають перевагу підручним низькотехнологічним методам для організації точкових, але при цьому ефективних терактів.

Як зазначає відомий американський дослідник тероризму Брюс Хоффман, терористи завжди намагатимуться залишатися на крок попереду антитерористичних заходів, пристосовуючись до технологічних змін, а їх атаки з часом будуть спрямовуватись не на добре захищені цілі, а на невиявлені слабкі місця інфраструктури держави [1]. Разом з тим, складність отримання терористами необхідних компонентів для вироблення ядерної, хімічної чи біологічної зброї масового ураження сприяє вибору найбільш доступних та консервативних засобів боротьби, оскільки більш екзотичні руйнівні засоби наражають терористів на більший ризик невдачі чи викриття. Саморобні