УДК 303.7
Куковинець О.Є.[1], Зайко Т.А.[2]
[1] студ. гр. КНТ-127 НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька Політехніка»

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ В БАНКАХ

Не буде перебільшенням сказати, що загроза умисних порушень функціонування автоматизованих систем обробки інформації в банках (АСОІБ) [1] різного призначення в даний час є однією з найбільших. Найбільш справедливо це твердження для країн, у яких потужна інформаційна інфраструктура, про що переконливо свідчать наведені нижче цифри.

Відомо, що в 1992 році збиток від комп'ютерних злочинів склав $ 555 млн., 930 років робочого часу і 15.3 року машинного часу. За іншими даними збиток фінансових організацій становить від $ 173 млн. До $ 41 млрд. на рік.

З прикладу вище, можна зробити висновок, що системи обробки і захисту інформації відображають традиційний підхід до обчислювальної мережі як до потенційно ненадійному середовищу передачі даних. Існує декілька основних способів забезпечення безпеки програмно-технічного середовища, що реалізуються різними методами.

Перший метод полягає в ідентифікації та авторизації за допомогою паролів. Завдання ідентифікації виконує незалежний сервер, який містить паролі, як для користувачів, так і для кінцевих серверів. Таким чином, використання мережевих послуг вимагає двох паролів, але користувач має знати лише один - другий надається йому сервером «прозорим» чином. Сервер стає вузьким місцем всієї системи, а його злом може негативно вплинути на безпечність всієї обчислювальної мережі. Після вдалої ідентифікації користувач авторизується у системі під своїм обліковим записом.

Другий метод полягає в інкапсуляції переданої інформації в спеціальних протоколах обміну. Використання подібних методів в комунікаціях засноване на алгоритмах шифрування з відкритим ключем. На етапі ініціалізації відбувається створення пари ключів - відкритого і

закритого, наявного тільки у того, хто публікує відкритий ключ. Ідея алгоритмів шифрування з відкритим ключем полягає в тому, що операції шифрування і дешифрування виконуються різними ключами (відкритим і закритим відповідно).

Третій метод полягає в обмеженні інформаційних потоків. Це відомі технічні прийоми, що дозволяють розділити локальну мережу на пов'язані підмережі і здійснювати контроль і обмеження передачі інформації між цими підмережами. До таких прийомів відносять Firewalls (брандмауери) та Proxy-servers.

Четвертий метод полягає у створенні віртуальних приватних мереж (VPN) [2], що дозволяють ефективно забезпечувати конфіденційність інформації, її захист від прослуховування або перешкод при передачі даних. Вони дозволяють встановити конфіденційний захищений зв'язок у відкритій мережі, якою зазвичай є інтернет і розширювати межі корпоративних мереж до віддалених офісів, мобільних користувачів, домашніх користувачів та партнерів по бізнесу.

П'ятий метод полягає у впровадженні систем виявлення вторгнень і сканерів уразливості, які створюють додатковий рівень мережевої безпеки.

Система виявлення вторгнень Cisco Intrusion Detection System (IDS) [3] може захистити мережу по периметру, мережі взаємодії з бізнес-партнерами і все більш вразливі внутрішні мережі в режимі реального часу. Система використовує агенти, що представляють собою високопродуктивні мережеві пристрої, для аналізу окремих пакетів з метою виявлення підозрілої активності.

Cisco Secure Scanner [3] являє собою програмний сканер промислового рівня, що дозволяє адміністратору виявляти і усувати уразливості в мережевій безпеці перш, ніж їх знайдуть хакери.

Підсумовуючи наведені методи, можна сказати, що розробка інформаційних систем вимагає паралельної розробки технологій передачі та захисту інформації. Ці технології повинні забезпечувати захист інформації, що передається, роблячи мережу «надійною», хоча надійність на сучасному етапі розуміється як надійність не на фізичному рівні, а скоріше на логічному (інформаційному рівні).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Демин В.С. Автоматизированные банковские системы [Текст] / В.С. Демин. – М: Менатеп-Информ, 1997. – 302 с.

2. Гайкович Ю.В. Безопасность электронных банковских систем [Текст] / Ю.В. Гайкович, А.С. Першин. – М: Единая Европа, 1994. – 605 с.

3. Загрози безпеці автоматизованих систем: [Електрон. ресурс]. – Режим доступу: http://www.modestbank.ru/bksys-752-1.html