

Застосування JSecureAPI для створення мереженої захищеної бази даних

Вступ. Сучасними тенденціями розвитку інформаційних технологій є яскраво виражений перехід у бік створення корпоративних інформаційних систем. При цьому основною характеристикою цих систем є обмеження доступу співробітникам корпорації до інформаційних та інших ресурсів обчислювальної системи. Причому дані тенденції виявляються практично для всіх рівнів ієрархії сучасних інформаційних технологій, починаючи з архітектурного рівня в цілому (Internet і Intranet), включаючи мережеві технології (наприклад, IP v.4.0 і IP Sec), і закінчуючи рівнем загальносистемних засобів (ОС, СУБД) і додатків.

Основна частина. Для вирішення завдання захисту інформації в системі локального, регіонального та глобального джекпотів мережі ігрових автоматів, в НВО «Vegas» на основі розробленої нами JSecureAPI були створені спеціалізовані бази даних для зберігання і обробки мережевих, глобальних і локальних даних [1].

В основі бібліотеки JSecureAPI лежать елементи методів захисту даних: стеганографії, одноразового блокнота, рандомізованого динамічного XOR.

Відповідно до методу захисту даних JSecureAPI формат запису в момент додавання запису в таблицю не визначений. Тобто, використовується технологія захисту, так звана «сіра пляма». Визначений тільки розмір запису в байтах. Для адресації даних використовується наступна схема (рис. 1).

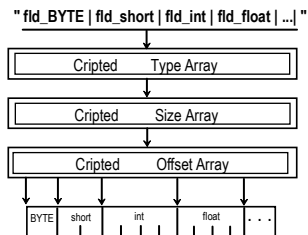


Рисунок 1 – Адресація даних «сірої плями» у файлі бази даних

Шифрація даних при записі здійснюється викликом методу `Jcrypt(data)`, а дешифрація – викликом методу `JUncrypt(pointer)` класу `Jcrypt`.

Висновки. Перевагою застосованого методу «сірої плями» в JSecureAPI для приховування даних є його надійність, простота та висока ефективність.

Література

1. Смирнов В. В. Система глобального джекпота сети игровых автоматов на территории Украины / В.В.Смирнов. Н.В.Смирнова / Отчет по НИР\ОКР – Кировоград, НПО «Vegas». 2004. – 428 с.

¹ кандидат технічних наук, доцент кафедри програмного забезпечення