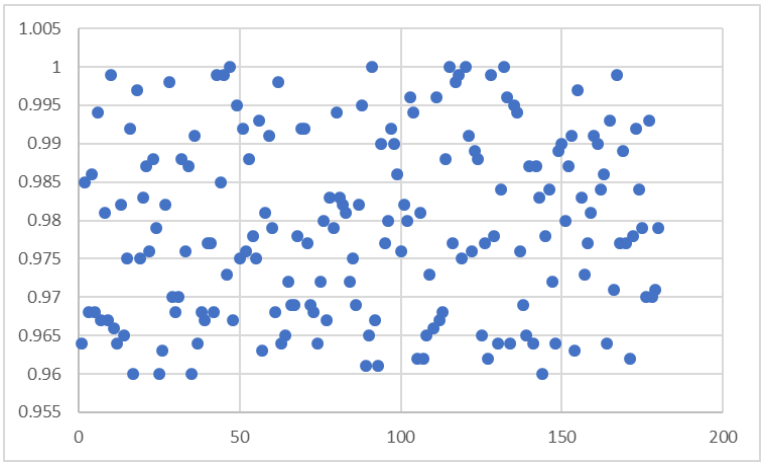

Рис. 1. Результати тестування послідовності згенерованої розробленим ГВЧ

На рис. 1 представлена діаграма, що характеризує попадання частки послідовностей, що пройшли кожен тест у довірчий інтервал [0,96; 1].

Отриманий результат підтвердив, що дана послідовність задовольняє відповідним критеріям випадковості.

Таким чином, за рахунок використання розробленого табличного ГВЧ, який враховує ентропію поведінки користувача, можна підвищити стійкість криптографічних алгоритмів, що, у свою чергу, сприятиме підвищенню захищеності Web-ресурсів.

УДК 004.056.52

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ МЕТОДІВ РОЗМЕЖУВАННЯ ДОСТУПУ В ІНФОРМАЦІЙНОМУ ПРОТИБОРСТВІ

Анатолій Шиян[1], Михайло Тюльпін[1], Яна Яремчук[1]
[1]Вінницький національний технічний університет,
[1]anatoliy.a.shiyan@gmail.com, mtyulpin@gmail.com, yanunova@hotmail.com

Інформаційне протиборство в глобальній мережі Інтернет зростає з кожним роком. З одного боку, економічне зростання йде за рахунок впровадження інновацій. З іншого боку, цінність конфіденційної інформації весь час зростає, що залучає до вимог отримати до неї несанкціонований доступ все більшу кількість зловмисників. Існує також і такий ускладнюючий фактор, що практично будь-яка інновація є результатом досить великого колективу. При цьому кожна людина із складу колективу є носієм певної частини конфіденційної інформації. До того ж,

доступ до конфіденційної інформації локалізований на членів колективу нерівномірно.

Таким чином, з точки зору доступу до конфіденційної інформації, в загальному випадку колектив є ієрархічною структурою. На вищих ієрархічних рівнях цієї структури знаходяться люди, які володіють більшим об'ємом інформації. У результаті цього захист інформації від несанкціонованого доступу вимагає використання спеціальних методів розмежування доступу.

Метою даної роботи є аналіз перспектив використання методів розмежування доступу в інформаційному протиборстві.

Методи розмежування доступу базуються на моделях керування доступом (Model Access Control). Вони описують в абстрактній формі способи розмежування доступу з фіксованим набором повноважень, враховують можливість видачі офіційних дозволів (допуску) суб'єктам до інформації різного рівня конфіденційності. Такі моделі поєднують захист з обмеженням прав на знайомство з певною інформацією та призначені для формування умов для протидії небажаному використанню інформації.

Моделі керування доступом мають такі обмеження:

● необхідність класифікації суб'єктів та об'єктів за рівнями безпеки, а це не завжди можливо у деяких системах;

● крім конфігурації розмежування доступом, також потрібна узгоджена політика безпеки, в якій має бути описано які об'єкти є захищеними об'єктами та які суб'єкти мають права доступу;

● користувачі системи не можуть одноосібно визначати доступ суб'єктів до об'єктів;

● серед параметрів керування доступом до об'єкту доступні лише категорії можливостей і мітки можливостей, котрі з ними пов'язані;

● доступом суб'єктів до об'єктів керують лише користувачі з правами адміністраторів;

● оскільки моделі керування доступом використовуються в поєднанні з іншими моделями контролю доступу, то часто важко з'ясувати, на якому «рівні» системи заборонено доступ, що вимагає більш тонкого налаштування усіх рівнів захисту.

Прикладом останнього обмеження є моделі дискреційного контролю доступу (Discretionary Access Control), які контролюють доступ до даного фрагменту інформації на основі політики, встановленої групою власників та/або уповноваженими членами колективу.

Перехід від абстрактних моделей до методів їх застосування завжди є одним із найважливіших етапів реалізації заходів інформаційного протиборства. На цьому етапі здійснюється імплементація теоретичної схеми, пристосовуючи її до умов реальної ситуації. Це можна здійснити, розробивши такі методи, які враховують специфічні особливості функціонування інформаційної системи того об'єкту, який потрібно захищати. Методи розмежування доступом орієнтовані перш за все на те, щоб захистити потрібну інформацію та інформаційні ресурси «зсередини» від власних співробітників.

Методи розмежування доступу, які впроваджені в організації, повинні враховувати не тільки існуючі на даний момент структуру інформаційних процесів

та інформацію, яка локалізована на певних співробітниках. Ці методи повинні бути орієнтовані на ті зміни, які виникають як при діяльності організації, так і виникають внаслідок зовнішніх причин.

До перших можна віднести те, що інформація може «дрейфувати» з часом, зменшуючи вимоги до свого рівня допуску. Наприклад, спочатку організація розробляє певний план дій. На початку, на рівні ідеї, цей план має найвищий рівень допуску. А коло людей, які мають доступ до відповідних документів, є вкрай обмежене. З часом ідея обростає документами, які розробляє досить велика кількість працівників. Ці документи вже будуть мати, як правило, менший рівень допуску. Нарешті, на етапі соціалізації ідеї, з результату розробки організації та її супровідних документів не тільки знімаються всі можливі рівні допуску, а й навіть створюються умови для максимально широкого розповсюдження інформації.

Зовнішні причини, які потрібно враховувати при імплементації моделей розмежування доступу та, розробляючи відповідні методи, методики та технології, мають високий рівень різноманітності та широке коли причин.

Наприклад, сторонні особи можуть впливати на співробітників організації різними способами. Найвідомішими прикладами є підкуп чи шантаж співробітників. Також сюди необхідно віднести і корупцію, яку часто намагаються відносити до внутрішніх причин, забуваючи, що при корупції співробітник організації може отримати зиск чи вигоду тільки і тільки за межами своєї організації. Тому зовнішні причини можуть просто полягати в тому, що сторонні особи будуть створювати умови для отримання зиску та/чи вигоди від порушення існуючого в організації розмежування прав доступу. Такий вплив, на відміну від підкупу чи шантажу, є передовсім виключно інформаційним, бо тут потрібно просто донести до співробітника організації ту інформацію, користуючись якою він може отримати певну вигоду.

Врахування перерахованих та інших умов і причин вимагає побудови спеціалізованих інформаційних технологій, які дозволять інформувати відповідні структури організації про порушення правил розмежування доступу. Такі інформаційні технології повинні стати невід'ємною складовою інформаційних потоків організації.

УДК 004.4.233 (043.2)

ІНСТРУМЕНТИ ДЛЯ ЗНЕВАДЖЕННЯ КЛІЄНТ-СЕРВЕРНИХ ЗАСТОСУНКІВ

Василь Буковецький[1], Юрій Тягур[2], Тетяна Матьовка[3]
Ужгородський національний університет
[1]bukovetsky@outlook.com [2]yurii.tjahur@uzhnu.edu.ua
[3]rtanyusha17@gmail.com

Розвиток технологій доступу до мережі інтернет дозволив створювати веб-застосунки, які по складності не поступаються повноцінним класичним програмним пакетам. Розробка застосунків, які виконують постійний обмін даними