Як видно структурна складність пропорційна квадрату порядку m поля Галуа та лежить приблизно в межах від S_{min} до S_{max}.

Висновок

У роботі зроблено аналітичну оцінку структурної складності помножувачів представлених в гаусівському нормальному базисі типу 2 елементів двійкових полів Галуа. Структурна складність пропорційна квадрату порядку m поля Галуа та лежить приблизно в межах від (1/2 … 3/4) m^2.

Список використаних джерел

1. В.С.Глухов., Р.М.Еліас, А.О.Мельник. Особливості реалізації на ПЛІС секційних помножувачів елементів полів Галуа $GF(2^m)$ з надвеликим степенем// "Комп'ютерно-інтегровані технології:освіта, наука, виробництво" - науковий журнал, Луцький національний технічний університет. № 12, 2013. С. 103 – 106.
2. Глухов В.С., Глухова О.В. Результати оцінки структурної складності помножувачів елементів полів Галуа//Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі" №773, 2013. С.27-32.
3. Глухов В.С. Особливості виконання операцій над матрицями в полях Галуа. Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи проектування. Теорія і практика". Вип. 564. Львів, 2006. С.35-39.
4. Hlukhov V., Hlukhova A. Galois field elements multipliers structural complexity evaluation. Proceedings of the 6-th International Conference ACSN-2013. September 16–18. – Lviv, 2013. – P. 18–19.

УДК 004.75

ЗАСІБ РОЗПОДІЛУ ДОСТУПУ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

Дубчак Л.О.[1)], Мамончук М.Ю.[2)]

Тернопільський національний економічний університет

[1)] к.т.н., ст. викладач; [2)] магістрант

Вступ

Для здійснення захисту даних в мережі існують багато методів. Основні з них протистоять несанкціонованому доступу до інформації [1]. Система захисту повинна враховувати рівень доступу клієнта, можливість проведення атаки під час передачі даних, а також працездатність самої комп'ютерної системи.

Захист конфіденційної інформації може здійснюватись шляхом вибору найоптимальнішого методу піднесення до степеня за модулем, що реалізується під час шифрування інформації. Крім того, варто застосувати апарат нечіткої логіки для побудови такої системи, оскільки вона дозволяє працювати в режимі реального часу [2, 3].

Метод розподілу доступу в комп'ютерній мережі

Суть пропонованого методу полягає в тому, що процес оброблення вхідної нечіткої інформації розділено на етапи навчання та експлуатації.

Під час навчання засобу оброблення нечіткої інформації визначено області функцій належності виходу для кожного з правил.

Під час експлуатації спочатку відбувається порівняння вхідних даних зі значеннями функцій належності виходу у визначених базою правил областях пам'яті, де зберігаються значення згаданих функцій належності виходу, відповідних до кожного правила нечіткого висновку. Далі відсікаються значення функцій належності виходу, які перевищують вхідні дані. Потім вибираються мінімальні значення функцій належності виходу, отриманих після відсікання, і будується з цих мінімальних значень відповідна фігура. Останньою операцією методу оброблення нечітких даних є пошук центра ваги фігури, отриманої в результаті додавання відсічених функцій належності виходу [4, 5].

Всі операції пропонованого методу близькі до операцій класичного механізму Мамдані і за складністю не перевищують їх. Однак кількість операцій у пропонованому методі менша, що сприяє зростанню його швидкодії [6].

Засіб розподілу доступу, реалізований в середовищі Simulink

Схема розробленого нечіткого контролера, що реалізує пропонований метод оброблення нечіткої інформації, подана на рисунку 1.

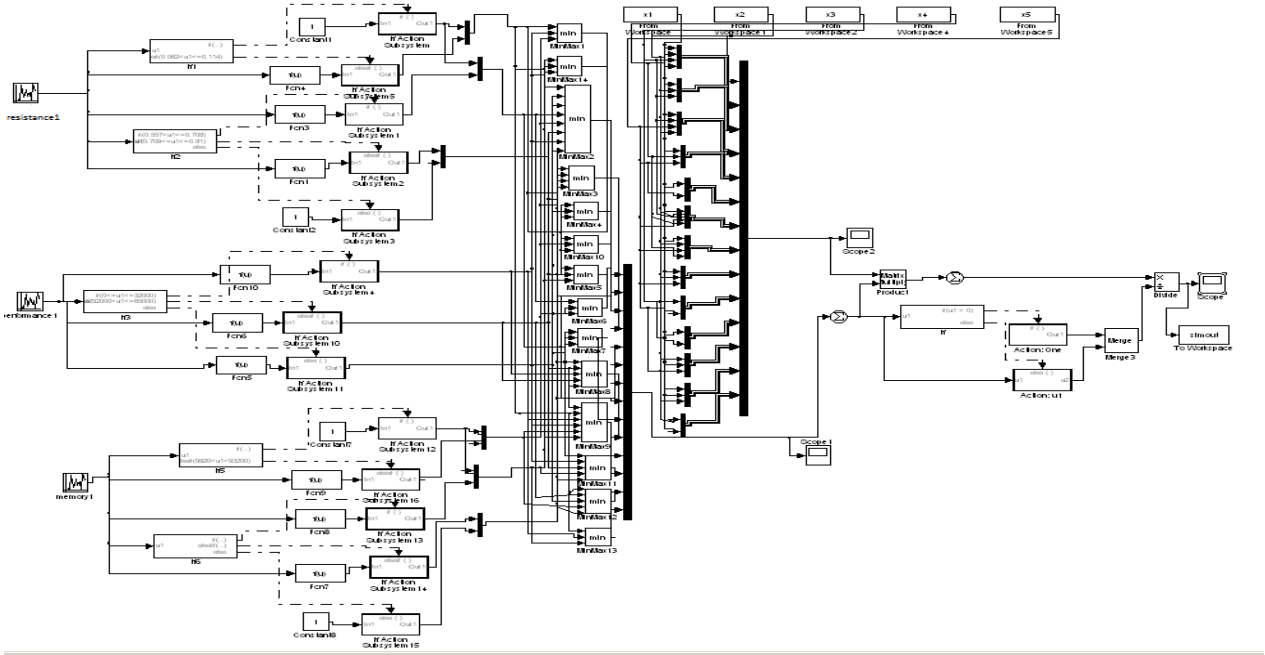

Рисунок 1 - Схема розробленого нечіткого контролера

Згідно схеми рисунку 1 спочатку здійснюється обчислення функцій належності вхідних змінних за допомогою блоків «if» та «function» середовища Simulink.

Вхідними змінними є стійкість системи до атаки під час передачі інформації поточному клієнту, продуктивність та можливі затрати пам'яті самої комп'ютерної системи. Виходом розробленого засобу є метод піднесення до степеня за модулем, що необхідно застосувати під час шифрування даних [7].

Для кожної області знаходяться мінімальні серед відповідних значень вхідних змінних, що реалізовано в схемі рисунку 1. Кінцева фігура описується абсцисами, що задаються з об'єднання виходів відповідних блоків «From Workspace», та ординатами, що відповідають виходам опрацювання функцій належності входів.

Тестові значення перевірки роботи схеми рисунку 1 подано в таблиці 1.

Таблиця 1

Тестові значення змінних розробленої нечіткої системи розподілу доступу в комп'ютерній мережі

№п\п	Resistance	Performance	Memory	Method
1	0.0452	1.68e+004	6.65e+003	3.64
2	0.0771	4.55e+004	9.31e+003	5.2
3	0.0239	6.2e+004	1.5e+005	4.81
4	0.104	3.64e+004	3.26e+005	7.25
5	0.157	7.85e+004	1.2e+004	3.91
6	0.604	6.3e+004	2.22e+005	6.4
7	0.96	9.49e+004	1.93e+005	1.93
8	0.0133	7.15e+004	3.99e+003	1.69
9	0.168	3.11e+004	3.5e+005	8.31
10	0.0452	2.95e+004	3.32e+004	2.65

Аналіз отриманих даних показує, що середнє відхилення результату роботи схеми запропонованого засобу розподілу доступу в комп'ютерній мережі від значення виходу нечіткого контролера за механізмом Мамдані становить мінімально 0,02 та 0,13 максимально, тобто в середньому 0,055, що підтверджує працездатність системи і правильність результатів.

Висновки

Запропонований засіб розподілу доступу в комп'ютерній мережі може застосовуватись в системах захисту інформації, що передається по відкритих каналах.

Список використаних джерел

1. Петров А.О. Принципи проектування та оцінки систем захисту інформації в мережах загального користування / А.О.Петров // Інформаційна безпека. – 2011. - №1(5). – С.49-56.
2. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы./ Д.Рутковская, М.Пилиньский, Л.Рутковский. - М.: Телеком, 2006. – 382 с.

3. Гнатчук Є.Г. Інформаційна технологія подання та опрацювання знань на основі нечіткої логіки в експертних системах діагностування комп'ютерних засобів: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.06 «Інформаційні технології» / Є.Г.Гнатчук. – Львів, 2008. – 20 с.
4. Дубчак Л.О. Метод обробки нечітких даних на основі механізму Мамдані /Л.О.Дубчак //Системи обробки інформації.– 2012. - №7(105). – С.131-134.
5. Дубчак Л.О. Спосіб обробки нечіткої інформації / Л.О.Дубчак // Вісник Східноукраїнського національного університету ім. В.Даля. – 2012. - № 8 (179), Ч.1. – С. 306-309.
6. Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данным / С.Д.Штовба // Проблемы управления и информатики. – 2007. – №4. – С. 102–114.
7. Дубчак Л.О. Спосіб вибору методу модулярного експоненціювання для побудови оптимальної системи захисту конфіденційної інформації / Л.О.Дубчак, Л.М.Тимошенко, Т.О.Яремчук // Інформаційна безпека – 2011. - №1(5). – С.112-116.

УДК 004.056.5

СОЗДАНИЕ СИСТЕМЫ РЕАЛИЗАЦИИ ФИШИНГОВЫХ АТАК С ЦЕЛЬЮ АНАЛИЗА МЕТОДОВ ЗАЩИТЫ

Жиляк А.Г.
Национальный технический университет Украины "Киевский политехнический институт", студент

I. Постановка проблемы

Новые информационные технологии широко внедрены во все сферы человеческой деятельности. Каждый пользователь желает иметь постоянный доступ к своей персональной и служебной информации, и быть уверенным в невозможности ее неправомерного использования.

При появлении угроз, связанных с возможностью потери, искажения, раскрытия конфиденциальных данных и утечке определенной информации, пользователь может стать жертвой злоумышленников, что приведет к отрицательным последствиям для пользователя (например, хищения крупных финансовых средств, раскрытие конфиденциальных данных и т.д.) . По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается и уровень угроз для используемых информационных технологий.

Одну из самых больших угроз информационной безопасности представляют именно методы социальной инженерии, хотя бы потому, что использование социального хакерства не требует значительных финансовых вложений и доскональных знаний компьютерных технологий, а также потому, что людям присущи некоторые поведенческие наклонности, которые можно использовать для осторожного манипулирования. На сколько бы не была автоматизирована и защищена информационная система, всегда будет присутствовать человеческий фактор (будь то преднамеренные или непреднамеренные действия), который нужно учитывать.

II. Цель работы

Целью данной работы является разработка программного продукта, с помощью которого можно осуществить фишинговую атаку с целью дальнейшей разработки комплекса защиты от атак данного рода.

III. Модель атаки

Для модулирования атаки был написан программный продукт, принцип работы которого следующий: на вход программы подается url-ссылка оригинального сайта, который при помощи wget клонируется. Затем в код html-страницы внедряется javascript, собирающий основную информацию с компьютера пользователя (местоположение, IPv4, IPv6, системное время, информация о браузере и операционной системе, HTTP-заголовки, информация о экране, навигатор и плагины — все эти данные отправляются на сервер), а так же обработчик формы ввода персональных данных, который их сохраняет и затем перенаправляет пользователя на оригинальный сайт.

На выходе программы получаем url-ссылку фишингового сайта. Клонированный сайт размещаем в "скрытом сервисе" в сети Tor. Ссылка фишингового сайта присылается обьекту атаки любым способом, используя сервисы по типу tor2web, которые позволяют обращаться к "скрытым сервисам" через обычный HTTP поддомен.