МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ
ЗВ'ЯЗКУ ІМ. О.С. ПОПОВА

ІНСТИТУТ КІБЕРНЕТИКИ ІМЕНІ В.М. ГЛУШКОВА

ПРОБЛЕМИ ІНФОРМАТИКИ ТА МОДЕЛЮВАННЯ

ТЕЗИСИ ШІСТНАДЦЯТОЇ МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(*12 – 16 вересня 2016 року*)

Харків – Одеса

2016

СЕКЦИОННЫЕ ДОКЛАДЫ

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ ШИФРОВАНИЯ ИНФОРМАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТЕВЫХ СООБЩЕНИЙ

канд. техн. наук, доц. А.И. Баленко, магистр Д.И. Глущук, НТУ "ХПИ", г. Харьков

Обоснована необходимость шифрования данных сетевых пакетов при передаче от клиента к серверу для сокрытия информации, передаваемой по линиям проводной и беспроводной связи.

К криптографическим алгоритмам должны предъявляться жёсткие требования в частности, к ключу, а также к самим процессам шифрования и дешифрирования для увеличения сложности вскрытия данных третьими лицами. Доказана необходимость использования комбинации из определённого количества стандартных алгоритмов шифрования, таких как md4, md5, SHA, DES, AES, так как увеличивает время для дешифрирования информации третьими лицами.

Доказана более высокая степень безопасности алгоритмов асинхронного шифрования, при которых не происходит обмен ключами, по сравнению с синхронными алгоритмами, при которых ключ для дешифрирования передаётся вместе с сообщением. Использование односторонних функций, алгоритма Диффи-Хеллмана сводит к минимуму возможность дешифрирования перехваченных данных и делает сам процесс очень ресурсоёмким и затратным по времени для третьих лиц.

Возникает необходимость пересмотра и модернизации классических алгоритмов авторизации, аутентификации, верификации, сетевого сообщения для возможности внедрения более сложных алгоритмов сокрытия информации. Доказана возможность применения прокси сервера вместе с шифрацией данных сетевых пакетов для контроля и повышения безопасности сетевого сообщения.

Применение прокси-сервера в средствах коммуникации позволяет повысить уровень безопасности удалённого управления поездами (на примере американской железнодорожной компании Amtrak) и предотвратить несанкционированный доступ к системе управления локомотивами.

Список литературы: **1.** Введение в криптографию. [Cryptography 101] – [Электронный ресурс] - http://citforum.ru/security/ cryptography/crypto_1.shtml. **2.** Асинхронные алгоритмы шифрования. Односторонние функции – [Электронный ресурс] https://intsystem.org/security/asymmetric-encryption-how-it-work/.

ПРИМЕНЕНИЕ НЕЧЕТКИХ ЛОГИК ДЛЯ МОДЕЛИРОВАНИЯ ПОКАЗАТЕЛЕЙ ТЕХНИЧЕСКОЙ ЭСТЕТИКИ

канд. техн. наук, проф. Е.Г. Бердичевский, НовГУ им. Ярослава Мудрого, г. Великий Новгород

Рассмотрена возможность моделирования важнейших комплексных показателей технической эстетики на основе теории нечетких логик и мягких чисел. В основу предлагаемой методики моделирования такого слабоформализуемого показателя как "эстетичность дизайнерского решения" положено использование одного из основных разделов нечетких логик – теории лингвистических переменных.

Лингвистическая переменная позволяет приближенно описывать явления и понятия, которые настолько сложны, что не поддаются описанию в общепринятых количественных терминах. Лингвистическая переменная определяется пятью параметрами:

$$(x, T(x), U, G, M),$$

где x – название переменной; $T(x)$ – терм-множество имен-значений переменной x. Каждому из этих имен соответствует подмножество X, заданное на универсальном множестве U с базовой переменной u; G – синтаксическое правило, порождающее имена значений переменной x (например, очень красивый, некрасивый, весьма красивый, очень некрасивый и т.д.); M – семантическое правило, ставящее в соответствие каждому элементу терм-множества нечеткое подмножество X универсального множества U. Такой подход позволяет строить так называемую функцию принадлежности нечетких подмножеств множества U с именами $T(x)$.

Основные понятия технической эстетики являются классическими лингвистическими переменными и их неопределенность может быть смоделирована аппаратом теории нечетких множеств. Предложена модель понятия "эстетичность" характеризовать 15-ю параметрами. Каждому параметру предлагается поставить в соответствие некоторое нечетное число, имеющее функцию принадлежности треугольной формы. Значение этого числа пронумеруем по принадлежности множеству $[o, a]$. Эти числа моделируют высказывание следующего вида; "параметр приблизительно равен $\bar{a}$ и однозначно находится в диапазоне $[o, a]$. В нашем случае $\bar{a}$ совпадает с $a/2$.

Такая формализация понятия "эстетичность" позволяет учесть не только содержательный аспект, но и этапность формирования эстетических показателей, т.е. выделить временной инвариант.

НАУКОВЕ ВИДАННЯ

ТЕЗИСИ ШІСТНАДЦЯТОЇ МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ "ПРОБЛЕМИ ІНФОРМАТИКИ ТА МОДЕЛЮВАННЯ"

Відповідальний за випуск к.т.н. М.Й. Заполовський

Науковий редактор д.т.н. Дмитрієнко В.Д.
Технічний редактор д.т.н. Леонов С.Ю.

Підп. до друку 02.09.2016 р. Формат 60x84 1/16. Папір Copy Paper.
Гарнітура Таймс. Умов. друк. арк. 5,30.
Облік. вид. арк. 5,0. Наклад 120 прим.
Ціна договірна

НТУ "ХПІ", 61002, Харків, вул. Фрунзе, 21

Видавничий центр НТУ "ХПІ"
Свідоцтво ДК № 116 від 10.07.2000 р.

Отпечатано в типографии ООО «Цифра Принт»
на цифровом комплексе Xerox DocuTech 6135.
Свидетельство о Государственной регистрации А01 № 432705 от 3.08.2009 г.
Адрес: г. Харьков, ул. Данилевского, 30. Телефон: (057) 7861860.