також те, що він може працювати і з іншими довжинами блоків даних та ключів. Хоча така можливість не входить до стандарту [3], проте вона може бути ефективно застосована на практиці.

Особливості програмної реалізації AES також випливають з особливостей самого алгоритма. Серед них, зокрема, слід відзначити нову архітектуру “Квадрат”, що забезпечує надшвидке “розсіювання” та “перемішування” інформації, при чому за один раунд перетворенню підлягає весь вхідний блок [5]. Крім того в алгоритмі застосовується байт-орієнтована структура, що під час програмної реалізації процесу шифрування забезпечує розробку на 8-розрядних мікроконтролерах. Варто відзначити одну з найважливіших особливостей AES: ефективна апаратна та програмна реалізація на різноманітних платформах. Зокрема важливим для програмної реалізації AES є те, що у структурі алгоритму закладена можливість паралельного виконання операцій, що на багатопроцесорних ЕОМ дозволить збільшити швидкість шифрування у кілька разів.

Список літератури

1. Тарасов О.В. Огляд та порівняльний аналіз методів стиснення інформації / О.В. Тарасов, Є.В. Онопко // Системи обробки інформації. – 2011. – Вип. 7 (97) – С. 64-67.
2. Бурачок Р.А. Використання симетричних алгоритмів шифрування при передаванні мультимедійних даних / Р.А. Бурачок, П.О. Гуськов, Р.І. Бак // Радіоелектроніка та телекомунікації. – 2012. – № 738. – С. 156-160.
3. Баричев С.Г. Стандарт AES. Алгоритм Rijdael / Баричев С.Г., Гончаров В.В., Серов Р.Е. // Основы современной криптографии. – М.: “ГЛ-Телеком”, 2002. – 247 с.
4. Дудикевич В. Б. Розробка клієнт-орієнтованих засобів шифрування абонентських даних в мобільному зв’язку / В.Б. Дудикевич, Ю.Л. Пархуць // Інформаційна безпека. 2011.–№1(5).–С. 83-87.
5. Фисун С.Н. Методика шифрования данных с использованием программно-методического комплекса VisualAES / С.Н. Фисун, А.И. Копылов // Радіоелектронні і комп’ютерні системи. – 2012. – № 5 (57). – С. 83-85.
6. Гаража В.О. Особливості програмної реалізації алгоритму AES / В.О. Гаража, О.П. Доренський // Актуальні задачі сучасних технологій: збірник тез доповідей Міжнародної науково-технічної конференції молодих учених та студентів, 19–20 грудня 2012 р., м. Тернопіль – Тернопіль: Вид-во ТНТУ ім. Івана Пулюя, 2012. – С. 184-185.
7. Основи захисту інформації: Навч. посібник. / [Смірнов О.А., Віхрова Л.Г., Осадчий С.І. та ін.]. – Кіровоград: РВЛ КНТУ, 2011. – 322 с.
8. Панасенко С.П. Алгоритмы шифрования. Спец. справочник / С.П. Панасенко. – СПб.: БХП Петербург, 2009. – 576 с.

УДК 004.4

Д.О. Давидов
Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи формування фільтрів від фішингу в мережі Internet

Найбільш розвинутою формою шахрайства в Інтернеті, безсумнівно, є фішинг. Зловмисники використовують перехоплювачі клавіатури, поштові повідомлення, складені за всіма правилами соціальної інженерії, спеціально розроблені сайти й інші засоби.

Усе більше винахідливими стають атакуючі, усе вище рівень їхньої підготовленості. Фішинг (phishing) – вид інтернет-шахрайства, що полягає в

розсиланні електронних повідомлень із метою крадіжки конфіденційної інформації (як правило, фінансового характеру).

Фішинг-повідомлення складаються таким чином, щоб максимально походити на інформаційні листи від банківських структур або компаній з відомими брендами. Листи містять посилання на свідомо помилковий веб-ресурс, спеціально підготовлений зловмисниками і є копією сайту організації, від імені якої відправлений лист.

На даному фальшивому сайті користувачеві пропонується ввести, наприклад, номер своєї кредитної карти й іншу конфіденційну інформацію.

Отже, розробка програмного забезпечення системи формування фільтрів від фішингу в мережі Internet є актуальною задачею, яка потребує розв'язку.

Список літератури

1. Гайкович В., Першин А., Безопасность электронных банковских систем. – Москва.: Единая Европа, 2002.
2. Галатенко В., Информационная безопасность, «Открытые системы». – М.: Азбука-Книга, 2005.

УДК 004.4

В.В. Джебко
Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи контролю та керування доступом з використанням смарт-карт за технологією RFID

Принцип комплексного «інтелектуального» управління всіма життєво важливими функціями житлових і промислових об'єктів, практична реалізація якого стала можливої завдяки застосуванню інтегрованих слабкострумових систем, знаходить сьогодні все більшу популярність.

Особливе значення при цьому мають спеціальні програмно-апаратні комплекси, призначені для забезпечення безпеки, і, насамперед, – системи контролю й управління доступом, або, скорочено СКУД.

Що являють собою системи контролю доступу? Загалом їх можна охарактеризувати як призначені для здійснення контролю й управління доступом як безпосередньо на об'єкт у цілому, так і на його окремі ділянки, комплекси, що поєднують у своєму составі організаційно-адміністративні заходи й великий перелік програмно-технічних засобів.

Крім властиво управління доступом з метою попередження проникнення на об'єкт небажаних осіб, функція системи контролю доступу може полягати також у спостереженні за обслуговуючим персоналом, включаючи пересування в межах території об'єкта, моніторинг періоду перебування на робочому місці, раціональність використання робочого часу й т.д. Установка систем контролю доступу й у житлових приміщеннях не менш затребувана, чим на господарських об'єктах, просто домашні системи, як правило, відрізняються більшою простотою й меншою кількістю інтегрувальних у їхній состав функціональних елементів.