УДК 004.056

Усач Н.В.
Кіровоградський національний технічний університет

Дослідження та програмна реалізація системи автентифікації користувача в мобільних пристроях

Одним із ключових завдань удосконалювання інформаційних комунікацій є завдання побудови безпечної інформаційної системи. Інтерес до неї обумовлений зростаючими обсягами конфіденційної інформації, переданої між учасниками інформаційного обміну, і швидким ростом таких показників інформації, як вартість втрати конфіденційності, вартість схованого порушення цілісності, вартість втрати інформації. Цій проблемі присвячена велика кількість наукових робіт і монографій. Захищеність комунікацій у безпечній інформаційній системі включає забезпечення конфіденційності й цілісності переданої інформації. Ці властивості забезпечуються використовуваними криптографічними системами, успішне функціонування яких припускає використання на приймальній й передавальній сторонах захищеного каналу криптографічних ключів, бінарних наборів достатньої довжини.

Для спрощення процедури генерації й розподілу секретних ключів у криптографії запропоновано й досліджено велику розмаїтість схем попереднього розподілу ключів. У них процедура доставки секретного ключа учасникам інформаційної системи виконується у два етапи: кожному учасникові довіреним центром доставляється пакет ключової інформації (у вигляді набору двійкових слів достатньої довжини), склад якого (у вигляді списку номерів і, можливо, деякої додаткової відкритої інформації про ці набори) публікується. При цьому кожний учасник, знаючи состави пакетів і опубліковані дані, може, використовуючи тільки набори зі свого пакета, обчислити для захищеної комунікації з будь-яким іншим учасником інформаційній системі ключ, що не може обчислити ніякий третій учасник.

Розвиток людської цивілізації супроводжується вражаючу уяву збільшенням обсягу створюваної, оброблюваної й збереженої інформації. Наприклад, по оцінці журналу ASAP, у світі щорічно з'являється близько 6 млрд. нових документів. По даним же Delphi Consulting Group, у цей час тільки в США щодня створюється більше 1 млрд. сторінок документів, а в архівах зберігається вже більше 1.3 трлн. різних документів. Слід зазначити, що потоки корпоративної інформації надзвичайно різноманітні за джерелами і формами її подання. Однак їх можна умовно класифікувати за формою зберігання: на електронні й паперові документи. Існують оцінки, що в цей час тільки близько 30% всієї корпоративної інформації зберігається в електронному виді (як у структурованому в базах даних, так і в неструктурованому). Вся інша інформація (близько 70%) зберігається на папері, створюючи чималі труднощі при її пошуку. Проте це співвідношення поступово міняється на користь електронної форми зберігання (зокрема, через розвиток систем електронних архівів). По даним Delphi Consulting Group, обсяг корпоративної електронної текстової інформації подвоюється кожні 3 роки. За прогнозом того ж журналу ASAP, до 2017 р. тільки близько 30% корпоративної інформації залишиться в паперовому виді, а 70% інформації буде зберігатися в електронному виді. Навряд чи, звичайно, коли-небудь всі документи стануть тільки електронними, однак безсумнівно, що електронна форма зберігання документів у перспективі буде переважати.

Ці вражаючі цифри й дані говорять тільки про те, що для будь-якого підприємства або організації питання оптимізації документообігу й контролю за обробкою інформації мають ключове значення. Це твердження можна підтвердити наступними даними. По оцінці Siemens Business Services, до 80% свого робочого часу керівник витрачає на роботу з інформацією, до 30% робочого часу співробітників іде на створення, пошук, узгодження й відправлення документів, кожний внутрішній документ копіюється, у середньому, до 20 разів і до 15%

корпоративних документів безповоротно губиться (при цьому, за даними журналу ASAP, середньостатистичний службовець витрачає щорічно до 150 годин свого робочого часу на пошук загубленої інформації). Існують також оцінки, що на роботу з документами доводиться витрачати до 40% трудових ресурсів і до 15% корпоративних доходів.

Саме тому ефективність управління підприємствами й організаціями не в останню чергу залежить від коректного рішення завдань оперативного і якісного формування електронних документів, контролю їхнього виконання, а також продуманої організації їхнього зберігання, пошуку й використання. Потреба в ефективному управлінні електронними документами й привела до створення систем електронного документообігу (СЕД).

В 70-х роках, коли почали створюватися автоматизовані системи управління, стало ясно, що ті самі дані про об'єкт використовуються в самих різних завданнях. Отже, ці дані потрібно виділити в окрему підсистему, що буде зберігати їх і забезпечувати доступ до них всім зацікавленим особам. Це дало поштовх до бурхливого розвитку систем управління базами даних (СУБД). Проектування баз даних і їхня організація являють собою сьогодні цілу галузь.

Звичайно дані, необхідні для рішення завдання (завдань), споконвічно перебувають на паперових документах, уводяться в комп'ютер і осідають у базах даних, звідки їх черпають різні програми. Ця технологія, цілком плідна, настільки в'їлася у свідомість, що вихідні документи стали здаватися якоюсь непотрібною сировиною, від якого не зле б відмовитися, особливо в майбутньому, коли візьмуть гору безпаперові технології, і дані будуть передаватися мережею від одного комп'ютера до іншого. Існували, щоправда, трохи незручні об'єкти начебто статей, тексти яких не цілком укладалися в поняття «даного» (реквізиту, атрибута, показника й т.п.), тому що не мали обмежень на довжину, та й звичайні операції (порівняння, пошуку й т.п.) з ними робити важко. Спочатку такі об'єкти просто не сприймалися, потім у базах даних для них стали виділяти спеціальні (так звані «memo») поля. Операцій з ними не передбачалося.

Однак, на початку 90-х років звична концепція роботи з даними перестала здаватися такий вже універсальною, а текстові документи, навпроти, уже дуже рідкими й специфічними. При цьому прорив відбувся відразу по декількох напрямках. Першу хвилю підняв Інтернет. Електронна пошта, величезна кількість доступних сайтів з найрізноманітнішою інформацією зажадали інший, ніж у СУБД, системи структуризації даних. «Повідомлення», HTML, XML, «пошукова машина» і т.п. – терміни із зовсім іншої області, ніж СУБД. Одночасно із цим почали розвиватися системи діловодства й контролю виконання розпоряджень. У цих системах поняття документа є основним, навіть якщо в реальності відбувається рухи тільки вторинної інформації – реєстраційних і контрольних карток. І нарешті, фундаментальне обґрунтування «документного» погляду на інформацію принесли спроби впровадження тієї самої безпаперової технології, що, здавалося, повинна була з ним покінчити. З'ясувалося, що для передачі мережею значимої інформації вона повинна бути «завірена» підписом. Але підпис, хоча б і електронний, ставиться не під якимось даним або набором даних, а тільки під документом, аналогом того самого, паперового. Коло замкнулося.

Таким чином, поступово формується ціла область – системи управління документами (СУД). Можна було б сказати – документообіг, і це було б правильно, але, на жаль, слово це розуміється часто в дуже вузькому змісті як якесь розширення діловодства. Область формується, хоча далеко ще не оформилася, не стала всім зрозумілою, «перевареною» у своїй особливості, із чітко вираженою концепцією, навкруги понять, завдань і т.п. Дещо з перерахованого вже досить пророблене, інше тільки починає усвідомлюватися.

Список використаних джерел

1. *Козлов М. Совершенствуем Делопроизводство // Cognitive Technologies. M. 1995. 124 с.*
2. *Документооборот. Прикладные аспекты // Сб. трудов ИСА РАН. Под ред. члена-корр. РАН Арлазарова В.Л. и д.т.н. проф. Емельянова Н.Е. – М.: Едиториал УРСС, 2004.*