УДК 004.02

ЗАДАЧІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ У СОЦІАЛЬНІЙ СФЕРІ

Т. М. Хомета

Українська академія друкарства,
вул. Підголоско, 19, Львів, 79020, Україна

Розглянуто технологію функціонування суспільства, що базується на обміні інформацією у всіх галузях діяльності людини, насамперед в управлінні суспільством. Визначено задачі інформаційного забезпечення в соціальному середовищі. Запропоновано методику права на безпеку функціонування у відповідному соціальному середовищі. Виявлено небезпеки різного типу, які появляються при переході системи управління суспільством від паперових носіїв інформації до електронних.

Ключові слова: *інформаційні технології, носії інформації, алгоритми шифрування, блоковий алгоритм DSS, шифр RSA, цифровий підпис, електронний носій, персоніфікація та ідентифікація даних.*

Постановка проблеми. На сучасному етапі розвитку інформаційного суспільства актуальними є питання інформаційної безпеки як окремої людини, так і держави загалом. З розвитком інформаційних технологій заміна носіїв інформації призвела до низки проблем, які стали актуальними у системі документообігу суспільства.

Мета статті — провести аналіз використання задач із переходом паперових носіїв інформації в електронні у соціальному середовищі.

Виклад основного матеріалу дослідження. Функціонування суспільства ґрунтується на обміні інформацією між окремими його представниками. Такий обмін поширювався на всі галузі діяльності людини, насамеред — на управління суспільством. Базовими засобами такого управління є документи, які мають характер управлінських чи різного типу рекомендацій, та регламентації видів діяльності для членів суспільства. З розвитком технологій інтенсивно почали змінюватися носії інформації: з паперового вигляду в електронний. Така зміна спричинила проблеми, які стали актуальними у системі документообігу у суспільстві. У переносному значенні папір матеріалізував інформацію, розміщену на ньому, що дає можливість доволі легко персоналізувати відповідні дані, ідентифікувати власників цієї інформації та розв'язувати задачі, пов'язані з використанням відповідної інформації. У зв'язку з цим виникли різні типи паперових носіїв:

– документи;
– паперові гроші;
– цінні папери;
– книги;
– листи та ін.

Кожна задача, пов'язана з управлінням суспільством, породжувала окремий клас паперових носіїв інформації у вигляді наказів, рішень, законів, різних

актів, що й створило базові засоби для реалізації в суспільстві юридичної системи. Управлінська система стосовно суспільства, яке формується на основі демократичних принципів, ґрунтується на використанні інформації, яка поширюється у соціумі, передається окремим його членам та надається на основі використання різних способів її передавання. Основний спосіб передавання інформації базується на використанні паперових носіїв. Очевидно, що управління суспільством здійснюється державними органами, кожен із яких орієнтований на певну сферу діяльності людей та задачі управління суспільством.

Розвиток інформаційних технологій, а особливо розвиток засобів електронного зв'язку між окремими джерелами інформації, що в багатьох випадках зреалізовані у формі електронних мереж, кардинально змінив можливості використання електронних носіїв інформації, які орієнтувалися на заміну паперових. Але сьогодні існують задачі, які необхідно розв'язати для перенесення усіх характеристик паперових носіїв інформації на електронні носії таким способом, щоб останні набули тих властивостей, якими вони відрізняються. До таких характеристик належать:

– простота використання двома сторонами, які обмінюються інформацією;
– легкість розв'язання задач, що ґрунтуються на використанні паперових носіїв;
– доступність усім членам суспільства так, як і паперових носіїв;
– юридична обґрунтованість використання електронних носіїв, що є основою певних гарантій для власників документів;
– можливість утилізації інформації, яка міститься на електронному носії;
– персоналізація електронного носія, та що відповідає можливостям персоналізації при використанні паперових;
– можливість оперативного отримання інформації, яка відповідає сприйняттю інформації з паперового носія, та інші властивості, що виникають на основі аналізу особливостей використання певної інформації.

У процесі функціонування суспільства існують загальні права, дотримання яких визначає певний тип суспільства. До них належать:

– право на приватне життя та його недоторканність у суспільстві;
– право на безпеку функціонування у відповідному соціальному середовищі та використання своїх можливостей на користь функціонування цілого середовища.

Наведені права є типовими для більшості соціальних середовищ і відображають, з одного боку, загальність відповідних правил, а з іншого — їх можливу суперечність.

У процесі переходу на електронні носії інформації право на приватне життя забезпечується засобами захисту, які, на відміну від використання паперових носіїв, є менш доступними для пересічного члена суспільства. Це пов'язано зі значними затратами на використання необхідних засобів. Приватні дані на паперових носіях інформації доступніші його власнику, на відміну

від електронних носіїв. Це означає, що виникає ризик їх підміни, що складніше виявити. Наприклад, документ, який ідентифікує особу з біометричними даними, не може бути перевірений без використання спеціального обладнання. Таким чином використання електронних документів дає ширші можливості підміни особистості.

Будь-який електронний носій відповідно до своїх функціональних властивостей може використовуватися у мережі: платіжна карта — у мережі здійснення платежів, документ ідентифікації особи — у базах даних державних установ, які стосуються реєстрації громадян і т. д. Це означає, що ідентифікаційні дані наражаються на небезпеку перехоплення, коли їх надсилають каналами передавання даних відповідної мережі.

Можна зазначити багато небезпек різного типу, які появляються у разі переходу у систему управління суспільством від паперових носіїв інформації до електронних. Сьогодні існує розвинена технічна дисципліна, де захищають інформацію, яку розміщують на електронних носіях [1–2]. Тому можна перейти від загального аналізу задач, що виникають у процесі використання електронних носіїв замість паперових, до конкретних задач, які в цьому випадку виникають. До них належать:

– захист даних, які розміщені на електронному носії;
– захист доступу до електронних носіїв;
– забезпечення інтегративних даних;
– забезпечення персонального доступу до інформації, розміщеної на електронному носії;
– створення багаторівневого захисту даних;
– забезпечення універсальності доступу до носія інформації під час її використання;
– зміна рівня захисту у часі використання носія ідентифікації та інші засоби, пов’язані зі специфікою використання відповідного носія даних.

Задача захисту даних є досить універсальною, а тому звузимо її розуміння до захисту від неуповноваженого зчитування даних чи заволодіння інформацією, яка міститься на електронному носії. Відомими, але досить загальними є методи використання шифрування даних, що полягають у заміні зрозумілого тексту кодами, які перетворити у відкритий текст може тільки уповноважена особа. Таке повноваження визначається наявністю у необхідного ключа розшифрування [3–4]. Існують й інші методи захисту відкритого тексту, наприклад, стенографічні методи. Найпоширенішими засобами для шифрування є блокові алгоритми шифрування та алгоритми шифрування із відкритим ключем. Блокові алгоритми використовують для шифрування текстів великого обсягу, оскільки останні є простішими у реалізації алгоритмів шифрування. Відомим блоковим алгоритмом є DSS. Алгоритми ґрунтуються на використанні бітових представлень закодованих літер та обернених алгоритмів перестановок бітів, а також на основі використання додавання бітових даних по модулю два та їх комбінацій. Відомою комбінаційною функцією цього типу є функція

Фейстеля. Кодові перетворення повідомлень дають можливість створити таку криптограму, яка являє собою зашифровані дані та яку важко, не маючи ключа шифрування, перетворити у відповідний відкритий текст.

Алгоритми шифрування, які ґрунтуються на використанні обчислень кодів тексту, реалізуються на основі використання медулярної арифметики. Такі алгоритми є несиметричними та використовують два ключі, один з яких є таємним, а інший — відкритим. В основі побудови таких алгоритмів є твердження та інші результати, отримані в теорії чисел [5]. Завдяки тому, що ці алгоритми використовують два ключі, за їх допомогою можна реалізувати цифровий підпис документа, функції якого є ідентичними до функцій звичайного підпису та полягають у ідентифікації автора. У разі формування цифрового підпису може використовуватися будь-який несиметричний шифр, зокрема шифри RSA, EeGamala й інші. Загальна схема цифрового підпису така: текст, що його необхідно підписати, перетворюється в код, який за допомогою односторонньої функції, або функції скруту, перетворюється в код, що має задані розміри й ідентифікує його. Таке кодування є відбитком прихованого повідомлення, аналогічним до відбитка пальця. Він шифрується за допомогою таємного ключа та передається адресату. При цьому відкритий текст може додатково шифруватися одним із блокових шифрів. Адресат відкритим ключем розшифровує скрут тексту і порівнює його з тим, який було розшифровано адресатом. Якщо два порівнювані коди однакові, то текст зберіг інтегральність і є незміненим, а той факт, що криптограму було розшифровано, підтверджує авторство відповідного тексту власника таємного ключа. Цифровий підпис часто використовують у механізмах обміну інформацією через електронні канали цифрової мережі.

Проблеми захисту приватного життя розглядають державні структури, які формують директивні документи, що визначають правила збору приватних даних і їх використання. Прикладом таких документів є дерективи, сформовані у вигляді кодексу використання приватної інформації. Їх суть загалом досить проста та полягає в:

– обмеженні збору інформації (збирати тільки необхідну персональну інформацію);
– отриманні даних безпосередньо від того суб’єкта, до якого вони належать, та інформуванні його про ціль збору відповідної інформації;
– використанні інформації лише в тих цілях, про які суб’єкту було повідомлено;
– забезпеченні суб’єкта можливістю захисту інформації приватного змісту та правом вимагати виправлення помилок.

Основою використання електронних носіїв інформації в межах задач управління суспільством є захист приватної інформації кожного з його членів.

Важливим завданням у галузі захисту даних є захист від неуповноваженого доступу. Річ у тому, що захист даних виконує свої функції, коли дані вибрані з бази даних, де вони зберігаються, але немає можливості ними скори-

статися. Захист доступу не дублює захисту самих даних, оскільки вони можуть передаватися каналами зв'язку, захист яких може виявитися недостатнім, та в процесі їх використання протягом тимчасового зберігання власником цих даних можуть реалізуватися неуповноважені спроби використання. Захист доступу ґрунтується на ідентифікації користувача. Методи ідентифікації користувачів, що використовуються в інформаційних системах, залежно від рівня безпеки системи застосовують засоби захисту різних рівнів складності. Найпростіший полягає у використанні ідентифікатора користувача та пароля. Ідентифікатор дає змогу вияснити, чи існує відповідний користувач у реєстраційній базі системи. Пароль являє собою таємний код, який відомий тільки користувачеві та є у базі паролів. На відміну від ідентифікатора, що його прийнято називати «логіном», пароль може відповідно до профілю захисту періодично змінюватися за запитом споживача.

Доступ ускладнюється у разі потреби підвищити рівень захисту доступу. Таке ускладнення реалізується у двох напрямах: ускладнюються механізми доступу, які дають можливість виявляти додаткові параметри користувачів, і формуються вимоги до надання користувачем додаткових ідентифікаційних даних. Прикладом таких розширень, які формуються для користувача, можуть бути впровадження відбитка пальця, розпізнавання голосових повідомлень, уведення рукописних знаків і т. д. З точки зору ускладнення алгоритмів аналізу, реалізуються алгоритми розпізнавання почерку роботи з клавіатурою, стиль користування системою, формування псевдообразу користувача і т. д. Більшість з наведених підходів орієнтовано на постійного користувача або на такого, що користується системою не менше заданого періоду часу. У разі перших користувачів система доступу, за умови високих вимог до рівня безпеки, здійснює глибший аналіз даних, які користувач уводить. Один зі способів підвищення рівня безпеки полягає у тому, що система доступу реалізує діалог, в межах якого може запропонувати користувачу графік процесу отримання доступу, пов'язаний з декількома окремими запитами до системи, які повинні виконуватися через певні інтервали часу. З наведеного опису видно, що методи підвищення рівня захисту доступу можуть мати різний характер як з боку системи, так і з боку користувача. Очевидно, що умови діалогу системи захисту з користувачем можуть мати різні сценарії залежно від вимог до рівня безпеки, який повинен забезпечити систему доступу.

Важливою задачею, характерною для роботи із соціальними системами, є персональний доступ до захищених даних. Вона виникає у випадку, коли користувач отримує захищений електронний документ. Тоді він повинен мати можливість зняти відповідний захист. Пересічний громадянин, який є простим користувачем, наприклад, системи Microsoft Office, не зможе самостійно використати алгоритм шифрування, щоб відкрити зашифрований текст. Це означає, що фрагмент системи електронного документообігу, який використовується в організації, що обмінюється документами з користувачем, повинен бути встановлений на комп'ютері користувача. Відповідний фрагмент має бути захи-

щений, оскільки його комп'ютер є приватним і не може використовуватися в таких самих умовах, як комп'ютери системи державної структури, що формувала відповідний документ. Наведена ситуація є суперечливою відповідно до загальної ідеї організації цифрового суспільства. Це ілюструє наявність однієї з задач, яку необхідно розв'язати в межах створення інформаційних систем для обслуговування соціальних середовищ. Сьогодні щораз частіше впроваджують документи для повсякденного користування, до яких належать ідентифікаційні документи, платіжні картки та ін. На них, окрім засобів захисту, розміщено персональні дані власника, які для забезпечення захисту є невидимими під час звичайного огляду відповідного документа. Його власник повинен мати можливість перевіряти свої дані, щоб виявити їх можливу підробку третьою стороною з метою заміни оригінального документа на підроблений. У такому разі ситуація з можливістю перевірки є досить складною, оскільки для зчитування прихованої інформації необхідно мати спеціалізовані засоби. Звертатися до уповноважених органів у зв'язку з підозрою є нераціонально, оскільки підозри є суб'єктивним фактором, а тому розв'язання цієї задачі є актуальним, бо інакше власник фальшивого документа може бути запідозрений у порушенні закону.

Інший аспект цієї задачі полягає у тому, що такі документи переважно мають багаторівневу систему захисту. Саме він визначає можливість перевірки власником свого документа на оригінальність. Власник використовує документ у тих випадках, коли виникає необхідність у ідентифікації особи. Не завжди особа, яка проводить перевірку, має можливість звірити дані, що мають усі рівні захисту. Це призводить до того, що в певних ситуаціях ідентифікувати себе може третя особа, яка використовує фальшивий документ або приховані дані такого документа. Прикладом такої ситуації можуть бути випадки несанкціонованого використання даних особи під час оримання коштів у банкоматі.

Ще однією задачею є впровадження електронних носіїв інформації в певне соціальне середовище. Вона відповідає врегулюванню відповідальності за захист даних, які захищено на різних рівнях. Це означає, що не може бути ситуації, коли всі дані з документа забезпечені одним рівнем захисту. Що стосується ідентифікаційних документів, то це забезпечується технічно. Наприклад, дані, які стосуються прізвища, імені, прописки тощо, є доступними для безпосереднього зчитування та захисту фізико-хімічними засобами. Інші — захищаються способами, які потребують спеціальних засобів для відкриття. Сьогодні є актуальною ситуація, коли для різних електронних носіїв інформації одного типу необхідні різні засоби зчитування інформації. При цьому реалізація алгоритмів доступу та й самі алгоритми можуть бути однаковими або відрізнятися між собою різними налаштуваннями. Коли йдеться про документи ідентифікації, то така ситуація може бути виправдана підвищенням рівня захищеності. Але якщо йдеться про документи, які з'являються в результаті співпраці громадянина з певною установою, то засоби зчитування прихованої інформації мають бути ідентифіковані до такої міри, яка не призвела би до зни-

ження рівня захисту документа, з одного боку, а з іншого — не потребувала би затрат, які перевищують вартість інформації. З цього постає завдання поширення або надання користувачеві даних, необхідних для відкриття захищеної інформації, яку не передбачається передавати користувачеві. Використовують відомі протоколи формування безпечних каналів, але в цьому випадку застосовувати їх недоцільно, оскільки вони є досить складними та потребують участі обох сторін, з яких одну представляє користувач, що може бути не готовим до участі в процедурі створення захищеного каналу.

У межах цієї проблеми виникає задача оперативного призначення класу таємності або деякого ідентифікатора захищеності, що повиннен бути забезпечений для відповідного типу даних. Сьогодні існує чотири класи захищеності для системи, однак цього недостатньо. Мало того, необхідна міра захищеності повинна однозначно зіставлятися із засобами захисту відповідної інформації. Ця задача в галузі захисту інформації не має загальноприйнятого розв'язання, оскільки це пов'язано зі складністю визначення міри стійкості або несанкціонованого усунення відповідного засобу захисту. Особливо це актуально щодо криптографічних алгоритмів [6].

Іншою задачею, яка потребує розв'язання в межах системи цифрового суспільства, є захист даних або інформації в часі. Відомо, що одним з параметрів, який характеризує стійкість засобів від зламання, під яким розумітимемо несанкціоноване їх відкриття, є час використання відповідних засобів захисту. Це зумовлено такими причинами:

– алгоритми злому засобів захисту постійно модифікуються, що пов'язано з необхідністю їх адаптації до модифікованих засобів захисту;
– внаслідок довготривалого використання того самого засобу захисту інформація про нього з часом поширюється і може стати відомою неуповноваженим особам;
– багаторазове використання того самого засобу захисту з однаковими параметрами дає можливість створити статистику, яка може бути використана для успішного несанкціонованого відкриття.

Необхідність захисту інформації, що стосується певних осіб, зумовлена тим, що у соціальному середовищі завжди існує небезпека, яка може ініціювати певну атаку на захищену інформацію. Така небезпека зазвичай накопичує відомості про вартість захищеної інформації, методи її захисту та ін. Ці дані уможливлюють легке несанкціоноване використання персональних даних у корисливих цілях. Прикладом може бути створення фірми на чужу особу, оформлення на неї та інших членів родини кредиту. Сьогодні основним захистом від цього типу атак є такі соціальні структури, як державні органи управління. Але їх функціонування є надзвичайно інертним і неефективним. Створення системи захисту на основі реалізації принципів формування цифрового суспільства є набагато ефективнішим і дешевшим порівняно з функціонуванням таких соціальних структур, як слідчі органи, судові системи і т. д. Наведені засоби захисту характеризуються неперервним функціонуванням у часі, яке

забезпечить необхідний рівень захисту, адаптуючись до змін, що відбуваються у соціальному середовищі. Аналогічна задача є актуальною і для систем захисту, що ґрунтуються на використанні алгоритмічних та технічних засобів. Це означає, що в межах цифрового суспільства потрібно розв'язувати задачі адаптації засобів захисту до змін, які відбуваються у суспільстві, та до змін вимог до рівня захисту, які виникають у результаті зміни вартості інформації.

Висновки. Запропоновано задачі, що існують в інформаційній соціальній сфері, проаналізовано різні аспекти процесу заміни паперових носіїв інформації на електронні, завдяки чому стало можливо сформувати нові задачі у виявленні різного типу небезпек від паперових носіїв інформації до електронних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Соколов А. В. Защита информации в корпоративных сетях / А. В. Соколов, В. Ф. Шаньгин. — М. : ДМК Пресс, 2002.
2. Сталлинг В. Основы защиты сетей. Приложения и стандарты / В. Сталлинг. — М. : Издательский дом «Вильямс», 2002.
3. Чмора А. Л. Современная прикладная криптографія / А. Л. Чмора. — М. : Гелиос АРВ, 2002.
4. Молдавян Н. А. Криптография: от примитивов к синтезу алгоритмов / Н. А. Молдавян, А. А. Молдавян, М. А. Еремеев. — СПб. : БХВ Петербург, 2004.
5. Петров А. А. Компьютерная безопасность / А. А. Петров. Криптографические методы защиты. — М. : ДМК, 2000.
6. Бабаш А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. — М. : СОЛОН-Р, 2002.

TASKS OF INFORMATION SUPPORT IN THE SOCIAL SPHERE

T. M. Khometa

Ukrainian Academy of Printing,
19, Pidholosko St., Lviv, 79020, Ukraine

The article examines the technology of society functioning based on an information exchange in all areas of human activity and above all things in the area of management of society. It determines the tasks of information support in the social environment. The law method on safety of functioning in the proper social environment has been offered. It also shows different types of dangers which appear in the case of transferring of the system of society management from the paper carriers to electronic data.

Keywords: *information technologies, carriers of data, algorithms of encoding, block algorithm DSS, code RSA, digital signature, electronic carrier, personification and identification of data.*

Стаття надійшла до редакції 11.09.2015.