2. Бухгалтерський словник / За ред. проф. Ф. Ф. Бутинця. – Житомир: ПП «Рута», 2001. – 224 с.

3. Бушуев С. Д., Бушуева Н. С., Бабаев И. А., Яковенко В. Б., Гриша Е. В., Дзюба С. В., Войтенко А. С. Креативные технологии управления проектами и программами: Монография. – К.: «Саммит-Книга», 2010. – 768 с.

4. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. і головн. ред. В. Т. Бусел. – К.; Ірпінь: ВТФ «Перун», 2005. – 1728 с.

5. Локк Д. Основы управления проектами / Пер. с англ. – М.: HIPPO, 2004. – 253 с.

6. Мазур И. И., Шапиро В. Д., Ольдерогге Н. Г. Управление проектами: Учебное пособие / Под общ. ред. И. И. Мазура. – 2-е изд. – М.: Омега-Л, 2004. – 664 с.

7. Словник іншомовних слів: тлумачення, словотворення та слововживання / За ред. С. Я. Єрмоленко. – Харків: Фоліо, 2006. – 623 с.

8. Управление проектами (Зарубежный опыт) / А. Кочетков и др.; Санкт-Петербургская академия недвижимости. – СПб.: Два Три, 1993. – 446 с.

9. Управління проектами (Керівництво з питань проектного менеджменту) – пер. з англ. / Під ред. С. Д. Бушуєва, 2-ге вид., перероб. – К.: «Деловая Украина», 2000. – 198 с.

Розломій І.О.

аспірант,
Черкаський національний університет
імені Богдана Хмельницького

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

В сучасному суспільстві використання електронних документів набуло широкого поширення в багатьох сферах людської діяльності. Використання систем електронного документообігу (СЕД) дозволяє отримати гнучкість при обробці документів, значно підвищити ефективність роботи всієї структури, для якої вони призначені. Впровадження СЕД для свого надійного функціонування передбачає створення специфічних методів та засобів захисту. Електронні документи вразливі до ряду загроз, насамперед до порушення цілісності, можливості несанкціонованого доступу та загрози модифікації. Модифікація спричинює фальсифікацію документа, яка може призвести до критичних ситуацій і стати причиною непередбачуваних наслідків. Захищений конфіденціальний електронний документообіг став необхідною умовою функціонування державних структур, підприємств та організацій.

Глобальна інформатизація усіх сфер діяльності людини, обсяг інформації, збереженої в електронному вигляді, зріс у тисячі разів. А з появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією цілісності інформації.

Останнім часом проблема захисту інформації загострюється у зв'язку із зростанням комп'ютерних злочинів, пов'язаних з підробкою електронних документів, що завдає шкоди фізичним та юридичним особам, а також

державним інтересам. Основна мета полягає у вирішенні важливої науково-технічної задачі підвищення рівня захищеності електронних документів.

Останнім часом вдосконаленням та розробкою дієвих засобів захисту інформації займалися такі науковці, як Панасенко С. П., Рудницький В. М., Молдовян А. А.

Проте, все ще залишається цілий ряд невирішених та недостатньо вивчених проблем у сфері захисту інформації. Основною задачею на сучасному етапі розвитку суспільства та його інформатизації є виконання вимоги постійного підвищення якості систем захисту інформації та оперативності обробки інформації. На сьогоднішній день вдосконалення та побудова нових криптостійких алгоритмів перетворення даних є одним із перспективних напрямів розвитку криптографії.

Мета дослідження – аналіз електронних документів, дослідження стандартного набору можливих загроз та перспектив розробки ефективних засобів захисту інформації.

Сучасний етап розвитку інформаційних технологій передбачає впровадження систем електронного документообігу (СЕД), що дозволяє значно полегшити діяльність органів державного управління, освіти, медицини, активізувати процеси в банківській, фінансово-комерційній та інших сферах людської діяльності. Про це свідчить і ринок систем електронного документообігу, який в останні роки стрімко зростає.

Проте даний процес неможливий без надійної системи захисту електронних документів і СЕД в цілому.

Системи електронного документообігу – автоматизовані системи, що забезпечують процес створення, управління доступом і розповсюдження великих обсягів документів у комп'ютерних мережах, а також забезпечують контроль над потоками документів в організації [1, с. 26].

До стандартних загроз електронного документообігу відносяться порушення цілісності – пошкодження та знищення інформації, спотворення інформації, загроза конфіденційності.

Цілісність документа – стан документа, при якому ні в змістовну, ні в реквізитного частини не вносилося ніяких змін. Модифікації в електроннму документі можуть бути випадковими і навмисними. Для захисту від випадкових змін, наприклад, втрати частини даних в результаті руйнування жорсткого диска, можна використовувати технології забезпечення відмовостійкості (резервування, дублювання даних), а також технології забезпечення безпечного відновлення (резервне копіювання інформації, використання електроннигх архівів). Для захисту від навмисних змін електроннигх документів методи криптографічного захисту інформації.

Шифрування саме по собі не забезпечує цілісність документа. Хешування являє собою процес перетворення за певним алгоритмом електронного документа в число певної довжини (хеш-код). При цьому незалежно від розміру електронного документа цей хеш-код завжди однієї і тієї ж довжини. Якщо електронний документ змінюється (випадково чи навмисно), то хеш-функція

теж обов'язково зміниться. По суті, хешування – це одна зі складових електронного підпису.

Захист електронних документів є однією з найбільш гострих проблем в інформатизації більшості сфер людської діяльності.

Захищеність СЕД характеризується рівнем безпеки. В загальному вигляді визначити стан рівня безпеки СЕД можна за допомогою моделі Белла-Лападули. Нехай, T – рівень конфіденційності, $R(r,w)$ множина прав доступу до системи, де r – доступ до читання, w – доступ до запису, n – послідовність прав доступу, i – послідовність рівнів конфіденційності стан ν називається досягнутим в системі $\sum=(\nu_0,R,T)$, якщо існує послідовність $\{(r_0,w_0),...,(r_{n-1},w_{n-1}),(r_n,\nu_n)\}:\mathrm{T}(r_i,w_i)$. Система $\sum=(\nu_0,R,T)$ є безпечною, якщо її початковий стан ν_0 – безпечний, і всі стани, досягнуті з ν_0 шляхом застосування кінцевої послідовності запитів із R – безпечні.

Основу СЕД складають електронні документи, які є вразливими до копіювання, різних видів модифікацій, фальсифікації, а також знищення. Тому, розробка методу, що дозволяє забезпечити достовірність, кофіденційність і цілісність електронного документа є першочерговим завданням.

Електронні документи мають різний рівень конфіденційності, тобто можуть мати повністю відкриту інформацію або інформацію для обмеженого кола користувачів. Крім того, виникає проблема забезпечення достовірності електронних документів. Одним із засобів забезпечення достовірності є електронний цифровий підпис. Проте, останнім часом, в зв'язку зі зростанням злочинів в інформаційній сфері, навіть ЕЦП не є гарантом надійності та достовірності документу. Електронний документообіг має супроводжуватися різними програмно-технічними засобами, що дозволять захистити документи від несанкціонованого доступу, випадкової чи навмисної модифікації.

Фальсифікації в електронних документах можуть призвести до непередбачуваних ситуацій в суспільних структурах. В зв'язку з потужними програмно-технічними можливостями підробки електронних документів, актуальною також є проблема розробки методів виявлення фальсифікацій в документах.

Збереження електронних документів передбачає комплекс заходів, щодо забезпечення надійності збереження даних, цілісність системи, а також програмно-апаратні рішення, що перетворює інформаційні ресурси в документи, які мають законодавчу силу.

Основу гарантування інформаційної безпеки в інформаційно-телекомунікаційних системах становлять криптографічні методи та засоби захисту інформації. Беручи до уваги те, що швидкісні криптографічні перетворення даних є найефективнішим засобом забезпечення таких характеристик безпеки інформаційних ресурсів, як конфіденційність і цілісність, то, безумовно, перспективним напрямком досліджень є розробка методів підвищення продуктивності криптографічних систем.

Криптографія є одним з найбільш потужних засобів забезпечення конфіденційності та контролю цілісності інформації. У багатьох відношеннях вона займає центральне місце серед програмно-технічних регуляторів безпеки. Проте, не варто забувати, що будь-який криптографічний алгоритм володіє такою властивістю як криптостійкість, тобто і для його захисту є певна межа [2, с. 114].

Особливе місце в електронному документообігу займає задача ідентифікації користувачів, вирішити яку покликаний електронний цифровий підпис (ЕЦП) – найбільш зручний сучасний інструмент для здійснення угод у віддаленому режимі та обміну юридично значимої документацією/ ЕЦП гарантує достовірність, забезпечує цілісність, дозволяє створювати корпоративну систему обміну електронними документами. Так само одним з головних достоїнств підпису є можливість удосконалити контроль за обігом, використанням та зберіганням електронної документації на підприємстві.

Сьогодні основним, і практично єдиним з запропонованих, рішенням для забезпечення достовірності документа є ЕЦП. Електронний цифровий підпис – засіб, який дозволяє, на основі криптографічних методів, встановити авторство і цілісність електронного документа. Для захисту і конфіденційності, і цілісності інформації необхідно використовувати в комплексі шифрування і ЕЦП.

Неконтрольоване поширення і застосування програмних засобів призводить до втрати конфіденційності інформаційних ресурсів громадян і держави в цілому. Як наслідок розвиток інформаційних ресурсів нерозривно пов’язаний з їх безпекою та захистом.

Проблема масового споживання фальсифікованих документів набула рис національного лиха і стає суттєвою загрозою для інтересів особистості, суспільства і держави, а, отже, для національної безпеки країни. Розробка засобів захисту документів від фальсифікації зараз є завданням державного масштабу.

Список використаних джерел:

1. Сабанов А. А. Некоторые аспекты защиты электронного документооборота // Connect! Мир связи. – 2010. – № 7. – С. 62–64.

2. Жданов О. Н. Методы и средства криптографической защиты информации: учеб. пособие / О. Н. Жданов, В. В. Золотарев; СибГАУ. – Красноярск, 2007. – 217 с.