РОЗРОБКА ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Чудінова Н. В., Ковальчук С. О., Крижановська О. Л., ЛДУ БЖД
НК – Кухарська Н. П., канд. фіз.-мат. наук, доцент, ЛДУ БЖД

В останні роки в Україні спостерігається перехід від традиційної (паперової) форми подання документів до електронної. Це дає змогу організаціям отримати відчутну економічну вигоду, оскільки переведення документообігу в електронну форму володіє низкою переваг, серед яких суттєве скорочення термінів створення і проходження документів у межах структури підприємства, спрощення процедури формування і передавання пакетів документів між підприємствами.

Не так давно в Україні був прийнятий закон “Про електронні документи та електронний документообіг” (від 22.05.2003 № 851-IV) [1], який встановлює основні організаційно-правові засади електронного документообігу. Відповідно до нього електронні документи, що складені з дотриманням чинного законодавства і підписані електронним цифровим підписом, мають таку ж юридичну силу як і паперові й в повній мірі можуть замінити їх.

Електронний документообіг передбачає, зокрема, реалізацію процедури передавання документів в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем [1]. Враховуючи сучасний стан, а також перспективи розвитку систем зв’язку і телекомунікацій, очевидним є широке використання для цих цілей відкритих каналів зв’язку, глобальних мереж. На відміну від паперового документу, який передається в єдиному екземплярі, копії електронних документів, що створюються під час передавання каналами зв’язку, можуть тривалий час зберігатися в електронних поштових скриньках суб’єктів документообігу та на серверах провайдерів. Доступ до звичайних документів можливий тільки фізично, безпосередньо в процесі їх передавання. У той же час, системи електронного документообігу надають їхнім користувачам набагато більше можливостей для реалізації доступу. Так, доступ до електронних документів, до того ж розтягнутий в часі на період зберігання електронних копій, може бути здійснений зловмисником віддалено без безпосереднього фізичного доступу до матеріальних носіїв. При цьому ні відправник, ні отримувач електронних документів можуть і не здогадуватися про наявність збережених копій і про факт несанкціонованого доступу до них, про перехоплення третьою особою вихідних електронних документів в процесі їх передавання.

Відповідно до чинного законодавства [1] суб’єктами електронного документообігу повинен забезпечуватися захист інформації з обмеженим доступом, якщо така міститься в електронних документах.

В умовах неможливості забезпечення абсолютного контролю каналів зв‘яку, з метою недопущення несанкціонованого доступу зі сторони третіх осіб, для захисту інформації під час передавання її відкритими каналами

можуть бути використані методи як криптографічного, так і стеганографічного захисту інформації.

При використанні криптографічних методів інформація деяким чином модифікується, перетворюється, у результаті чого приховується зміст повідомлення [2]. Стеганографічні методи приховують сам факт передавання або зберігання інформації [3-5]. Це досягається шляхом впровадження її в різні мультимедійні об'єкти (контейнери), які при цьому не втрачають своїх споживчих властивостей. Варто зауважити, жоден із двох перелічених напрямків на нинішньому рівні їх розвитку не в стані самостійно вирішити усі завдання, пов’язані з захистом інформації, у тому числі, у сфері електронного документообігу. Вирішення низки завдань специфічного характеру можливе тільки за умови сумісного узгодженого використання методів криптографії та стеганографії. В основі, перспективного на сьогодні, криптостеганографічного підходу лежить ідея попереднього шифрування інформації з подальшим прихованням отриманої криптограми в контейнері.

Предметом наших досліджень є визначення шляхів і способів протидії, небезпечних для інформаційної безпеки підприємства, діям інсайдерів; розробка механізмів забезпечення прихованості від потенційних конкурентів найбільш важливої для підприємства частини електронного документообігу; розробка гібридних (на основі тісної взаємодії та синтезу криптографічних і стеганографічних методів) схем програмної реалізації алгоритмів захисту від несанкціонованого доступу до електронних документів під час передавання їх відкритими каналами зв’язку.

Розроблені нами в рамках проведених досліджень програмні засоби криптостеганографічного захисту конфіденційних повідомлень можуть бути використанні при проектуванні нових, а також вдосконалені існуючих автоматизованих систем електронного документообігу, а також інших систем захищеної передачі інформації відкритими каналами локальних та глобальних мереж.

ЛІТЕРАТУРА

1. Закон України від 22.05.2003 р. № 851-IV “Про електронні документи та електронний документообіг” за станом на 06 листопада 2014 року.
2. Задірака В. К. Комп’ютерна криптологія : підручник / Задірака В. К., Олексюк О. С. – К. : Вид-во “Збруч”, 2002. – 504 с.
3. Аграновский А. В. Стеганография, цифровые водяные знаки и стегоанализ : монография / Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С.А. – М. : Вузовская книга, 2009. – 220 с.
4. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Изд-во “Солон-Пресс”, 2009 – 272 с.
5. Конахович Г. Ф. Компьютерная стеганография. Теория и практика. / Конахович Г., Пузыренко А. – К. : Изд-во “МК-Пресс”, 2006. – 280 с.