server-cloud/windows-server/virtual-desktop-infrastructure.aspx. − Title from screen.

[13] LTSP Linux server terminal projekt [Electronic resource]. − Mode of access: http://wiki.ltsp.org/wiki/Concepts. − Title from screen.

В статье сделан анализ метода построения информационно-коммуникационных систем на основе терминальной системы, определены позитивные и негативные стороны терминальных систем в целом и особенности их использования в государственных учреждениях Украины, очерчены перспективы внедрения терминальных систем при создании информационно-коммуникационных систем в архивной отрасли.

Ключевые слова: процесс информатизации, информационно-коммуникационная система, терминальная система, терминальный сервер, тонкий клиент, информационная безопасность.

This article analyzes the method of creation information-communication systems based on terminal system. Identify positive and negative aspects of terminal systems in general and of the use in states institutions of Ukraine. Determined by the prospects of using terminal systems to create information - communication systems in the archives of Ukraine.

Key words: informatization process, information-communication system, terminal system, terminal server, thin client, information security.

УДК [005.92:004.63]: 681.188

Вадим Малиновський

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ КРИПТОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Розглянуто особливості застосування програмної та апаратної реалізації криптографічних засобів захисту електронних документів відповідно до вимог законодавчої бази України щодо захисту електронних документів, окреслено перспективи розвитку криптографічних засобів захисту електронного документообігу.

Ключові слова: системи електронного документообігу, електронний цифровий підпис, криптографічні засоби захисту електронних документів.

Нині майже не існує систем електронного документообігу, які б не містили засобів криптографічного захисту інформації (далі – КЗІ), зокрема засобів, що дають змогу використовувати в електронному документообігу електронний цифровий підпис. Слід зазначити, що й сам електронний цифровий підпис отримують за результатом криптографічного перетворення набору електронних даних, як визначено у ст. 1 Закону України «Про електронний цифровий підпис»[1].

Однак, як для суб'єктів захисту електронних документів, так і для розробників засобів криптографічного (далі – криптозасобів) захисту їх ще й дотепер не вирішено низку проблем:

– створення об'єктивної, оптимальної системи оцінок безпеки електронних документів та криптографічної стійкості засобів шифрування і електронного цифрового підпису;

– вдосконалення методів та способів ефективної апаратної і програмної реалізації криптографічних алгоритмів;

– розробка високоефективних систем криптоаналізу для дослідження сучасних систем криптозахисту даних[2];

– створення інформаційних систем у державних архівах та формування підходів і вимог до забезпечення їхньої безпеки.

Метою статті є аналіз сучасних криптозасобів захисту електронних документів, а саме – їх шифрування, накладання електронного цифрового підпису, та визначення перспективних напрямів дослідження зазначених методів і засобів захисту електронного документообігу.

Безсумнівно, основним позитивним показником засобу КЗІ є його криптостійкість, але в більшості практичних завдань при виборі криптографічних алгоритмів особливий інтерес становляють не тільки кількісні показники їхньої ефективності, а й функціонування у різних критичних умовах – загрозах, спектр яких при сучасних досягненнях науки та техніки може бути дуже широким.

Засоби КЗІ можуть мати апаратний, програмно-апаратний, або програмний спосіб реалізації. А тому низка критеріїв – надійність, якість, продуктивність та ін. – залежатиме від способу

їхньої реалізації. Наприклад, для розробників засобів захисту критерієм може бути економічна ефективність, яка є співвідношенням отриманої користі від затрачених ресурсів[3].

Найнадійнішими криптосистемами є ті, що засновані на апаратних засобах КЗІ. Вони реалізуються на основі програмованих та апаратно-орієнтованих процесорів. Апаратно-програмні та програмні засоби з точки зору криптографії переваг перед апаратними засобами КЗІ не мають[4].

Проблеми ефективної реалізації апаратних криптозасобів в Україні досліджували Т. А. Коркішко[5], Я. Р. Совин[6] та ін. У США способи реалізації криптографічних методів захисту публікуються в фаховому виданні «The Journal of Cryptographic Engineering (JCEN)», яке виходить із квітня 2011 р. В Україні та інших країнах СНД аналогічних видань поки що немає.

Тепер активно досліджується проблема вразливості й атак на кінцеві реалізації криптоалгоритмів через побічні канали витоку інформації. Серед вітчизняних учених, що вивчають її, найбільший інтерес викликають праці Я. В. Решетаря і В. В. Хоми[7].

Апаратні засоби КЗІ пропонується поділяти на такі групи[8]:

– засоби виконання криптографічних алгоритмів;

– засоби виконання криптографічних функцій;

– засоби виконання криптографічних протоколів.

Указані засоби дають змогу здійснювати таке[9]:

– реалізувати тільки необхідні функції апаратури;

– максимально підвищити швидкість опрацювання даних[10];

– забезпечити належний захист від побічних електромагнітних випромінювань;

– реалізувати вимоги до міцності виробу;

– забезпечити санкціонований доступ до вузлів апаратури, ключам та постійній інформації, що зберігається в електронних модулях;

– використовувати модульний принцип компонування криптозасобів;

– виготовляти окремі зразки апаратури за індивідуальними замовленнями.

Для оцінки ефективності апаратної реалізації алгоритмів одним із основних критеріїв є кількість і складність елементарних операцій, які необхідно виконати. Під ефективністю реалізації, передусім, будемо розуміти виконання критеріїв максимальної швидкодії, мінімальних затрат ресурсів, обсяг пам'яті, споживання електроенергії при достатньому рівні криптостійкості та надійності[11].

На нашу думку, ключовою проблемою при розробці апаратних засобів є відсутність вимог вітчизняних стандартів до виробів такого типу, тому доводиться користуватися критеріями та вимогами, визначеними у стандартах інших країн. Прикладом такої реалізації може слугувати засіб Д-300, призначений для криптографічного захисту конфіденційної інформації, що є власністю держави та передається по первинних цифрових каналах типу Е1, а також вироби серії ОНіКС-50,100 Науково-впроваджувальної фірми «Криптон», які при включеному живленні автоматично виконують низку тестів, зокрема тести американського стандарту FIPS 140-2[12].

Програмні засоби шифрування є реалізацію одного або декількох криптоалгоритмів на мові програмування високого або низького рівня, у вигляді модулів, бібліотек, окремих програм із функцією криптографічного захисту[13].

Проблеми ефективної реалізації, вимоги та підходи створення програмних засобів захисту інформації досліджуються в працях О. М. Бевза[14], О. В. Казарина[15] і Д. В. Склярова[16].

Технологія реалізації криптоалгоритмів програмними засобами має низку особливостей[17]:

– необхідність додаткового контролю за якістю функціонування, оскільки роботу програмного засобу КЗІ порушити легше, ніж апаратного аналогу;

– можливість контролю помилок в закритому тексті при шифруванні шляхом введення надлишковості;

– необхідність забезпечення надійного зберігання ключів;

– можливість масштабування і доповнення засобу КЗІ новими програмними блоками і модифікаціями вже використовуваних;

– принципова можливість використання програмного засобу КЗІ з відкритим кодом, що допускається при шифруванні інформації в приватних цілях.

Програмний засіб криптографічного захисту інформації незалежно від реалізованого криптоалгоритму має низку особливостей шифрування[18]:

– файли, зашифровані програмним засобом КЗІ, можуть зберігатися на інших носіях автоматизованої системи;

– розмір блока в блочному алгоритмі може перевищувати розмір сегмента файлу, через що розмір останнього збільшується;

– швидкість шифрування програмними за-

собами може бути нижчою, ніж апаратними, за рахунок завантаження центрального процесора криптографічними обчисленнями;

– робота з ключами ускладнюється через відсутність апаратної ідентифікації користувачів.

Для успішного проходження сертифікації програмний засіб захисту повинен обов'язково відповідати певним критеріям, зокрема вимогам безпеки.

Вимоги до програмних засобів КЗІ встановлюються нормативними документами. В кожній країні розробляються власні нормативні документи з цього напряму діяльності, найчастіше – стандарти. В Україні – це нормативні документи системи технічного захисту інформації: НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»[19] та НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»[20], в яких детально описано методи оцінки функціональних послуг безпеки, що забезпечуються з використанням криптоалгоритмів та ЕЦП.

Відповідно до нормативних документів з інформаційної безпеки, вимоги до програмного забезпечення поділяються на функціональні і гарантійні. Функціональні вимоги забезпечують протидію загрозам безпеці, а гарантійні вимоги забезпечують довіру до того, що програмний засіб коректно спроектовано і розроблено.

Безпека програмного забезпечення в широкому розумінні є властивістю цього програмного забезпечення функціонувати без прояву різних негативних наслідків для конкретної інформаційно-телекомунікаційної системи[21].

До функціональних вимог безпеки програмного засобу КЗІ відносять вимоги[22]:

– до криптографічної підтримки;
– до реалізації сервісів (послуг);
– до керування доступом;
– до захисту об'єктів;
– до самотестування;
– до генерації випадкових чисел;
– до налаштування середовища.

Склад та структура засобів криптографічного захисту електронних документів залежить від призначення системи електронного документообігу, середовища функціонування та наявності документів з обмеженим доступом. Засоби КЗІ застосовуються не тільки в захищених системах, де є потреба в високому рівні конфіденційності, а й в системах, де є певні вимоги до забезпечення цілісності, ідентифікації та автентифікації, наприклад, у системах електронного документообігу органів виконавчої влади.

Зараз майже в усіх системах електронного документообігу є підсистема захисту інформації, складовою якої є програмні та апаратні засоби криптозахисту, що забезпечують:

– надійну ідентифікацію та автентифікацію з використанням сучасних методів криптографії;
– використання електронного цифрового підпису;
– шифрування документів.

Нині провідними виробниками засобів захисту в Україні є Науково-виробничий центр «Безпека інформаційних технологій і систем» (м. Київ), Товариство з обмеженою відповідальністю (далі – ТОВ) «БЕСТ ЗВІТ» (м. Київ), Науково-впроваджувальна фірма «Криптон» (м. Київ), Акціонерне товариство «Інститут інформаційних технологій» (м. Харків) та ін.

Нормативна база, що регламентує криптографічний захист електронних документів, включає:

– нормативно-правові акти України;
– міжнародні стандарти;
– національні стандарти країн, криптозасоби яких сертифіковані в Україні (останні стандарти використовуються як рекомендаційні при розробці вітчизняних засобів захисту).

Одним із перших документів у галузі криптозахисту в Україні став указ Президента України від 22.05.1998 р. № 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні»[23], який регулює порядок застосування криптозасобів для захисту різних видів інформації з обмеженим доступом.

Нині основними документами, що регламентують розроблення та виготовлення апаратних, програмних та апаратно-програмних засобів криптографічного захисту, є накази адміністрації Державної служби спеціального зв'язку та захисту інформації «Про затвердження Положення про порядок розроблення, виробництва та уведення в експлуатацію засобів криптографічного захисту конфіденційної інформації, що є власністю держави» від 22.04.2008 р. № 82/ДСК та «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації» від 20.07.2007 р. № 141[24]. Відповідно до вимог останнього документа, засоби КЗІ класифікуються за такими характеристиками:

– за способом реалізації;
– за конструктивним виконанням;

– за призначенням.

Він також визначає:

– рівні можливостей порушника та необхідні класи засобів КЗІ, що обираються з урахуванням цих рівнів;

– вимоги до принципів побудови засобів КЗІ та технічної реалізації криптографічних алгоритмів у засобах КЗІ;

– вимоги до криптографічних засобів;

– вимоги і норми щодо захисту засобів КЗІ від витоку інформативних сигналів каналами побічних електромагнітних випромінювань та наведень.

Порівняння вітчизняної нормативної бази (не враховуючи керівні документи, що мають гриф обмеження доступу) із закордонною дає підстави зробити висновок, що в законодавстві України немає низки документів, які дали б змогу унормувати деякі важливі питання щодо засобів КЗІ. Серед закордонних документів є такі:

білоруський стандарт СТБ34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации», в якому детально викладено функціональні та гарантійні вимоги безпеки до програмних засобів КЗІ;

стандарти США серії FIPS PUB 140, в яких сформовано вимоги до апаратного або програмного забезпечення, що зашифровує та розшифровує дані або виконує інші криптографічні операції[25];

наказ Федеральної служби безпеки Російської Федерації від 27.12.2011 р. № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра»[26] (відповідно до вимог цього документа засоби електронного підпису та засвідчувального центру класифікуються згідно з їхніми можливостями протистояти атакам з урахуванням усього життєвого циклу даних засобів).

На нашу думку, враховуючи особливості вітчизняного законодавства, передовий досвід інших країн та досягнення вітчизняних й закордонних учених у галузі криптології, актуальним питанням є розроблення власних стандартів, в яких було б детально викладено вимоги до технічної реалізації як криптозасобів у цілому, так і засобів електронного підпису. Ця проблема вже частково порушувалася у працях вітчизняних науковців[27].

Отже, нами вище оглянуто функціональні особливості апаратних та програмних засобів захисту інформації та їхню роль при організації захисту електронних документів, запропоновано низку напрямів, що вимагають подальшого дослідження, а саме:

– розроблення методик комплексної оцінки криптозасобів захисту електронних документів;

– техніко-економічне обґрунтуваня та оптимізація криптографічних підсистем захисту електронних документів як складових комплексних систем захисту інформації;

– удосконалення нормативних документів, що регламентують вимоги до програмних і апаратних виробів, в яких реалізовано криптографічні функції.

[1] Про електронний цифровий підпис: Закон України від 22.05.2003 № 852–IV // Офіц. вісн. України. – К., 2003. – № 25. – Ст. 1175.

[2] *Лупенко С. А., Луцків А. М.* Моніторинг та керування обчислювальними процесами у сучасних кластерних системах під час розв'язання задач криптоаналізу // Вісн. Нац. ун-ту «Львівська Політехніка». – 2011. – № 717. – С. 76–83.

[3] *Скляров Д. В.* Искусство защиты и взлома информации. – СПб.: БХВ-Петербург, 2004. – 288 с.: ил.

[4] *Мухачев В. А., Хорошко В. А*. Методы практической криптографии. – К.: ООО «Полиграф-Консалтинг», 2005. – 215 с.

[5] *Коркішко Т., Мельник А., Мельник В.* Алгоритми та процесори симетричного блокового шифрування. – Львів: БаК, 2003. – 168 с.; *Мельник А., Коркішко Т.* Методика проектування багатоканальних процесорів симетричного блокового шифрування // Вісн. Терноп. держ. техн. ун-ту. – 2002. – № 2. – С. 100–109.

[6] *Совин Я. Р., Хома В. В., Решетар Я. В.* Реалізація криптографічного алгоритму згідно з ДСТУ ГОСТ 28147:2009 для вбудованих систем на базі ARM-процесорів // Вісн. Нац. ун-ту «Львівська Політехніка». Комп'ют. системи та мережі. – 2012. – № 717. – С. 158–167; *Совин Я. Р., Решетар Я. В., Хома В. В.* Електронний безпровідний ідентифікатор для доступу до ПК // Вісн. Нац. ун-ту «Львівська Політехніка». Автоматика, вимірювання та керування. – 2010. – № 665. – С. 39–44.

[7] *Решетар Я. В., Хома В. В.* Вразливості кінцевих реалізацій криптоалгоритмів до атак через побічні канали витоку інформації // Інформ. безпека. – 2009. – № 2. – С. 119–127.

[8] *Мельник А., Морозов Ю., Мельник В., Коркішко Т.* Проблеми і тенденції розвитку апаратних засобів захисту інформації // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2002. – Вип. 5. – С. 158–162.

[9] *Мухачев В. А., Хорошко В. А.* Методы практической криптографии. – С. 198.

[10] Методы и средства криптографической защиты информации: учеб. пособие / Федер. агентство по образованию, Сиб. гос. аэрокосмич. ун-т им. академика М. Ф. Решетнева; авт. кол.: О. Н. Жданов, В. В. Золотарев. – Красноярск: СибГАУ, 2007. – 217 с.

[11] *Астапенко Г. Ф.* Аппаратно-програмные методы и средства защиты информации. – Минск: БГУ, 2008. – 188 с.: ил.

[12] Каталог продукції науково-впроваджувальної фірми «Криптон» [Електронний ресурс]. – Режим доступу: http://www.crypton.ua. /index.php?id=15 – Назва з екрана.

[13] Методы и средства криптографической защиты информации. – С. 202.

[14] *Бевз О. М., Квєтний Р. Н.* Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальноювідстанню: монографія / ВінНТУ. – Вінниця, 2010. – 96 с.

[15] *Казарин О. В.* Безопасность программного обеспечения компьютерных систем: монография. – М.: МГУЛ, 2003. – 212 с.

[16] *Скляров Д. В.* Искусство защиты и взлома информации. – 288 с.: ил.

[17] *Жданов О. Н., Золотарев В. В.* Методы и средства криптографической защиты … – С. 208.

[18] Там же. – С. 209.

[19] Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу: НД ТЗІ 2.7-009-09. – [Чинний від 2009-07-24]. – К.: Адміністрація держспецзв'язку, 2009. – 171 с. – (Нормативний документ системи технічного захисту інформації).

[20] Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу: НД ТЗІ 2.7-010-09. – [Чинний від 2009-07-24]. – К.: Адміністрація держспецзв'язку, 2009. – 131 с. – (Нормативний документ системи технічного захисту інформації).

[21] *Казарин О. В.* Безопасность программного обеспечения компьютерных систем. – С. 5.

[22] Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации: СТБ 34.101.27-2011 / Белорус. гос. ун-т, Науч.-исслед. ин-т приклад. проблем математики и информатики. – Взамен: СТБ П 34.101.27-2007; действителен от 2012-03-01. – Минск, 2011. – 32 с. – (Госстандарт Республики Беларусь).

[23] Про Положення про порядок здійснення криптографічного захисту інформації в Україні: указ Президента України від 22.05.98 № 505/98 // Офіц. вісн. України. – 1998. – № 21. – Ст. 4.

[24] Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації від 20.07.2007 № 141 // Офіц. вісн. України. – 2007. – № 56. – Ст. 44.

[25] Security Requirements for Cryptographic Modules: FIPS PUB 140-2 / Federal Information Processing Standards Publications Information Technology Laboratory National Institute of Standards and Technology. – Gaithersburg, Issued May 25, 2001.

[26] Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра: приказ Федеральной службы безопасности Российской Федерации от 27.12 2011 г. № 796 // Собрание законодательства Российской Федерации. – 2011. – № 15. – Ст. 2036; № 27. – Ст. 3880.

[27] Див., наприклад: *Горбенко І. Д., Шапочка Н. В., Козулін О. О.* Обгрунтування вимог до генераторів згідно з ISO/IEC 18031 // Радіоелектронні і комп'ютерні системи. – 2009. – № 6. – С. 94–98; *Мартиненко С. В., Андреев Ю. Ю.* Требования надежности средств создания ЭЦП // Моделювання та інформаційні технології: зб. наук. пр. / Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України. – 2005. – № 29. – С. 153–161.

Рассмотрены особенности применения программной и аппаратной реализации криптографических средств защиты электронных документов в соответствии с требованиями законодательной базы Украины к защите электронных документов, обозначены перспективы развития криптографических средств защиты электронного документооборота.

Ключевые слова: системы электронного документооборота, электронная цифровая подпись, криптографические средства защиты электронных документов.

Consider the features hardware and programmatic implementation of cryptographic protection of electronic documents in accordance with the legislation of Ukraine to protect electronic records. Outlines the perspective of improvement of cryptographic protection of electronic documents circulation.

Key word: electronic documents circulation, electronic digital signature, cryptographic protection electronic records.