УДК 621.391.7:336.71(075.8)

В.К. Задирака, А.М. Кудин, В.А. Людвиченко, А.С. Олексюк

О технологии криптографической защиты информации на специальных цифровых носителях

Исследованы вопросы разработки новой технологии реализации средств криптографической защиты информации, адекватных современным технологиям распределенной обработки данных. Введено новое понятие специальных цифровых носителей информации, позволяющее рассматривать с единой точки зрения защиту электронных документов различного типа. Рассмотрены аспекты применения технологии для терминальных мобильных устройств обработки информации. Предложена математическая модель средства защиты, реализованного по данной технологии. Предполагается, что использование данной модели позволит получать формальное доказательство стойкости систем защиты информации.

The problems of the development of a new technology of the implementation of cryptography modules, adequate to the distributed data processing are researched. A new concept of the special digital media is introduced, allowing to consider the protection of electronic documents of various type from the uniform point of view. The aspects of application of the technology for terminal mobile devices of the information processing are considered. A mathematical model of the protection means implemented according to the given technology is suggested. It is supposed that the use of the given model will allow to receive a formal security proof of the information protection systems.

Досліджено питання розробки нової технології реалізації засобів криптографічного захисту інформації, адекватних сучасним технологіям розподіленої обробки даних. Введено нове поняття спеціальних цифрових носіїв інформації, що дозволяє розглядати з єдиної точки зору захист електронних документів різного типу. Розглянуто аспекти застосування технології для термінальних мобільних пристроїв обробки інформації. Запропоновано математичну модель засобу захисту, реалізованого за цією технологією. Є припущення, що використання даної моделі дозволить отримувати формальний доказ стійкості систем захисту інформації.

Введение. Основными тенденциями развития информационно-телекоммуникационных систем в настоящее время являются: стандартизация и унификация технологии обработки информации на основе принципа открытых систем; интеллектуализация систем обработки информации; миниатюризация средств обработки информации; интеллектуализация средств ввода/вывода информации и повышение их эргономичности; повышение мобильности телекоммуникационных технологий и программного обеспечения, а также энергонезависимости средств обработки информации.

Эти тенденции определяют приоритетное развитие следующих технологий:

- *Web* – технологии доступа к неструктурированным, распределенным, гипертекстовым данным;
- распределенных вычислительных систем [1] с распределенным хранением и обработкой информации; основу этих технологий составляют методы *облачных вычислений* [2], краткий обзор которых приводится далее, и сетевые структуры данных [3] (в частности – распределенные файловые системы);
- технологий виртуализации [4];
- гибридные, масштабируемые и «интеллектуальные» телекоммуникационные системы [1].

Остановимся на некоторых из этих технологий. *Облачные* вычисления – это новая концепция взаимодействия потребителя вычислительных услуг с вычислительной средой. Если предыдущие технологии предоставляли для обработки данных традиционные вычислительные ресурсы, то при облачных вычислениях предоставляемым в общее пользование ресурсом является программное обеспечение (так называемая технология «*SaaS*» (*Software as a Service*) [2]). Основой облачных вычислений является интеллектуальная телекоммуникационная система, виртуализация всех вычислительных ресурсов и стандартизация интерфейсов запросов и протоколов взаимодействия с вычислительной средой. С точки зрения потребителя вычислительных ресурсов вычисления становятся масштабируемой услугой [2], связанной

только с абстрактными вычислительными единицами (*юнитами*), а не традиционными вычислительными ресурсами. Прикладной программе пользователя предоставляется возможность гибко получать ресурсы по запросу, что есть новым уровнем абстракции вычислений от ресурсов вычислительной системы в сравнении с уровнем виртуальной машины. Параллельно с развитием технологий распределенных вычислений развиваются методы распределенного хранения данных, среди которых особо следует отметить создание масштабируемых хранилищ данных с неструктурированными запросами, например на основе *Google BigTable* [3].

Новые принципы и технологии построения информационно-телекоммуникационных систем (ИТС) определяют новые принципы и технологии их защиты [5]. В частности, дальнейшее развитие распределенного хранения данных и вычислений приводит к необходимости создания полностью автоматических систем защиты передаваемой информации на канальном уровне модели взаимосвязи открытых систем (модели ВОС) и к масштабируемым системам защиты – на сетевом и прикладном уровнях модели. Эффективными методами защиты при этом являются только криптографические методы защиты информации. Особенно эффективны данные методы для защиты различных электронных документов или их хранилищ. Заметим, что специфические требования защиты электронных документов (множество форматов, разные требования по атрибутам защиты и, соответственно, отсутствие необходимости использования всего сервиса защиты) определяют актуальность разработки технологии криптографической защиты, ориентированной именно на защиту распределенных электронных документов.

Возможность построения такой технологии исследовалась в работах [6, 7]. Существующие тенденции развития ИТС и их систем защиты показали, что задача дальнейшего развития предложенной технологии чрезвычайно актуальна. Так, применение многих из возможных современных технологий сдерживается отсутствием адекватных им технологий защиты информации [8], а существующие модели распределенных вычислительных систем разрабатываются в основном для оценки их производительности и надежности [9]. Практической иллюстрацией этому служит предпринятая попытка разработки в Украине единого формата электронного документооборота [10]. При этом формат разрабатывался только с учетом требований по обработке информации и слабо ориентирован на защищенную обработку документов, в частности не рассмотрены проблемы автоматического назначения грифа документа, категории доступа, подписи содержания документа вне зависимости от формата его представления и т.д. Фомальные модели, описывающие безопасную обработку этих документов (с учетом введенных показателей состояния конфиденциальности и целостности документов) предложены не были. С другой стороны, последние работы в области построения защищенных ИТС и систем электронного документооборота [6, 7, 11] могут составить основу для разработки таких моделей. Далее рассмотрим развитие технологий [6, 7].

Специальные цифровые носители информации и их функции

Анализ технологии обработки электронных документов – аналогов бумажных бланков *строгой отчетности* и ценных бумаг различного типа (электронные деньги, электронные ценные бумаги, цифровые паспорта) позволяет выделить общие для всех данные, наличие которых необходимо для организации защищенного взаимодействия с этими электронными документами. Согласно Закону Украины «Про електронний документообіг», устанавливающему цифровую подпись как обязательный элемент электронного документа, такими общими данными будут обладать все электронные документы. Таким образом, содержание электронного документа и информация, относящаяся к формату его представления «погружаются» на своего рода носитель информации, определяющий правила защищенного взаимодействия с документом. Поэтому логично эти структуры определить как *специальный цифровой носитель информации*. Отсюда следует, что специальные цифровые носители информации (СЦН) являются электрон-

ными документами специального типа с определенным интерфейсом доступа к ним, и потому могут сохраняться на любых носителях информации.

Наиболее удобны для указанных целей терминальные устройства хранения и обработки информации: интеллектуальные карты (интеллектуальные пластиковые карты с памятью, рис. 1), токены (рис. 2), смартфоны, коммуникаторы и нетбуки [12], другие мобильные вычислительные *гаджеты*. Среди СЦН информации особенно выделим цифровые паспорта (удостоверение личности), предназначенные в частности для идентификации и аутентификации личности. Как правило, для хранения цифрового паспорта применяются гибридные носители, позволяющие отображать визуальную информацию, которую можно прочитать невооруженным глазом, и машиносчитываемую информацию, размещаемую в специальном микрочипе, вмонтированном внутри паспорта.

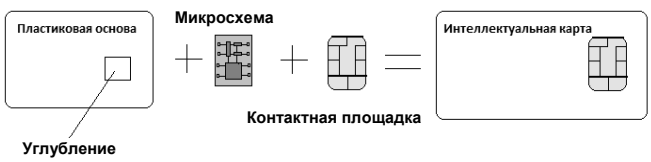


Рис. 1

Рис. 2

Наиболее известные терминальные устройства хранения и обработки информации – интеллектуальные карты (ИК) [13].

Интеллектуальная карта **(***smartcard* **–** смарт-карта**)** – это пластиковая карта со встроенным специализированным вычислительным устройством, состоящим из процессора, постоянного и оперативного устройства памяти под управлением специализированной операционной системы. Благодаря встроенному микропроцессору ИК имеют широкие возможности защищенного хранения и обработки информации.

Области использования ИК:

• банковские операции (дебетные и кредитные карты, сберегательная книжка и др.);

• идентификационные операции (удостоверение личности, паспорт, удостоверение водителя и др.);

• медицинское обслуживание (медицинский «паспорт», карты обязательного и добровольного страхования);

• торговые системы (дисконтные карты, карты предварительно оплаченные и пополняемые и др.);

• системы контроля доступа (в помещение, компьютерные сети и пр.);

• многофункциональные прикладные использования.

USB-ключ **(*брелок*, *токен*)** – электронное устройство хранения и обработки информации, выполненное в виде брелока, подключаемого к *USB*-порту непосредственно или с помощью кабеля. Фактически токен есть ИК в другом варианте физического выполнения (так называемом форм-факторе) и с другим интерфейсом передачи данных.

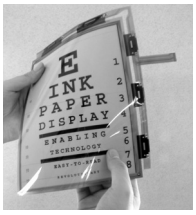
Гибкость в выборе форм-факторов токенов в сравнении с ИК определяет их потенциально большие технологические возможности при использовании более производительных микропроцессоров, большего объема памяти и дополнительных специализированных микросхем [14].

Коммуникаторы и смартфоны, нетбуки и другие вычислительные мобильные «гаджеты» – это самостоятельный класс вычислительных средств, которые по своим функциональным возможностям и форм-фактором занимают промежуточное положение между смарт-картами и ноутбуками. Нетбуки позволяют достичь времени автономной работы в несколько десятков часов, гаджеты с вводом/выводом по технологии электронной бумаги [15] (рис. 3)– до нескольких суток активной работы.

Криптографические технологии защиты информации на СЦН

При реализации средств защиты информации, сохраняемой на цифровых портативных интеллектуальных носителях и в распределен-

ных вычислительных системах возникают следующие проблемы:



Микрокапсулы-пикселы

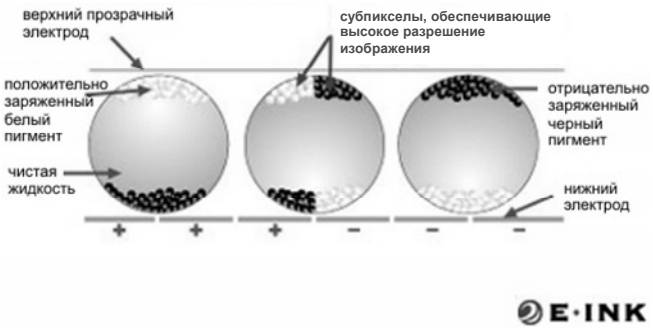


Рис. 3

• непосредственное использование криптографических технологий, применяемых для традиционных носителей информации, приводит к возникновению новых каналов утечки информации;

• недостаточное развитие теории формального синтеза криптосистем приводит к практической сложности формального доказательства стойкости полученных реализаций к криптоанализу;

• существующие технологии не используют методов защиты, естественных для распределенного хранения и обработки данных, таких, как рассечение/сбор.

Таким образом, существующие технологии реализации средств защиты информации на цифровых носителях, таковы: стандарты описания функциональности защиты электронных документов (подмножества *XML – SGML* и др.); технология безопасности *Java*-машины для унификации безопасного выполнения универсального кода; стандартизация криптографических примитивов; стандартизация реализации криптографических механизмов (низкоуровневые интерфейсы, определенные стандартом *PKCS* #11, интерфейсы среднего уровня – *CAPI*, *CNG*, высокого уровня – *GCS–API*, *GSS–API* и др.); требования по безопасности криптографических модулей, определенные стандартом *FIPS* 140–2 не ориентированы на использование на цифровых носителях информации.

Существующие технологии [16], в частности технологии *BSAFE RSA* фирмы *Data Security*, *PGP Disk*, *BestCrypt* фирмы *Jetico*, *DriveCrypt* продолжают развиваться в следующих направлениях:

• постепенный переход от технологии криптографической защиты отдельных файлов или записей в информационных хранилищах к защите специальных носителей информации (защищенных логических дисков) и областей оперативной памяти;

• создание универсальных по интерфейсам (*PKCS*#11, *Microsoft CRYPTOAPI* и др.) и реализации (под разные операционные системы, с использованием технологий *Java* или аналогичных ей) средств криптографической защиты информации;

• переход от обособленных реализаций функций конфиденциального и целостного хранения данных (так называемых *цифровых сейфов*), к полным по функциональности логическим аналогам средств криптографической защиты информации, которые руководствуются выбранной политикой безопасности (например, так называемая концепция *Policy-Based Approach* фирмы *RSA Data Security*).

Таким образом, стойкие тенденции развития средств криптографической защиты информации (СКЗИ) состоят в том, что на прикладном уровне модели взаимосвязи открытых систем (ВОС) с многообразием протоколов обработки данных применяются многофункциональные, мобильные и переносимые программно-аппаратные решения с четким разделением на функциональную (реализующую требуемые функции защиты) и жизнеобеспечивающую (хранения критических данных, необходимых для работы, и системы обеспечения целостности) части. Как правило, – это модули, соответствующие стандарту *FIPS* 140–2, но требующие высокой квалификации от разработчика систем защиты в связи с необходимостью интеграции

в платформу и построения систем управления ключами. На сетевом и канальном уровнях модели ВОС – это максимально автоматизированные устройства шифрования трафика, возможность построения которых определяется существованием достаточно формальных спецификаций протоколов. Поэтому следует сосредоточиться на задаче реализации многофункционального средства СКЗИ и сделать его распределенным и максимально автоматизированным. Отдельно рассмотрим решение задачи автоматизированного процесса разработки СКЗИ для терминальных устройств, отдельно для облачных распределенных вычислительных систем, учитывая факт, что применяемая модель защиты должна согласовываться с моделью распределенной вычислительной системы. Как будет показано далее, эти задачи могут быть решены с использованием одной и той же технологии.

Практически речь идет о новом подходе в технологиях реализации криптографических средств защиты данных, которые сохраняются, а именно – создание «программной прослойки», реализующей все необходимые криптографические механизмы защиты независимо от программно-аппаратной платформы реализации этих механизмов.

Характерный пример таких технологий – технология цифрового сейфа. Идея создания цифровых сейфов (как и ее развитие – создание виртуальных интеллектуальных карт) берет начало в традиционном подходе абонентской шифровки файлов. Известно, что в некоторых операционных системах любое физическое устройство ЭВМ представляется файлом специального вида. С помощью такого подхода можно образовать логический (виртуальный) накопитель любого типа, чтение/запись к которому осуществляется чтением/записью информации в файл. Если программное обеспечение, осуществляющее чтение/запись к логическому диску дополнительно при каждой операции осуществляет расшифровку/шифровку информации, то при отключении накопителя информация в файле зашифрована («замкнута» в виртуальный «сейф»). Для данных, сохраняемых на таком защищенном виртуальном диске, к свойству их конфиденциальности обычно добавляются функции обеспечения подлинности, целостности и других свойств безопасности. Такой подход реализован в программных продуктах многих известных фирм (*RSA Data Security*, *PGP Corporation*, *Jetico*, Ланкрипто и др.), а некоторые продукты компании Ланкрипто даже получили и соответствующее название – «Криптосейф».

Новый подход в технологиях реализации криптографических средств защиты данных позволяет полностью отделить развитие средств обработки данных от средств их криптографической защиты и создать универсальную программную платформу для защиты любых электронных документов. Один из примеров преимущества такого подхода – решение проблемы цифровой подписи электронных документов независимо от способа их представления (кодировки, формата и пр.). Заметим, что классическим аналогом такого универсального защищенного носителя есть бланки документов строгой отчетности с элементами технологической защиты (например, бумага с водяными знаками).

Идея заключается в следующем. Вводится понятие «универсальный цифровой защищенный носитель» как технология, которая состоит из:

- универсального программного интерфейса для прикладных программ (подобно *Microsoft CRYPTOAPI*);
- множества атомарных программных модулей (например, *Java*-апплетов) реализации криптографических (стеганографических) примитивов обработки блоков данных (шифрование, выработка цифровой подписи, вычисления хешкода, вычисления имитовставки, вычисление примитива аутентификации, внедрение цифрового водяного знака, верификация цифрового водяного знака и др.);
- неупорядоченного набора атомарных данных, которые могут быть расположены на любом физическом носителе и в любом месте распределенной вычислительной системы (как в защищенном, так и открытом виде);

• *XML*-шаблона электронного документа, который и определяет конкретный тип документа (цифровой паспорт, электронные деньги, электронная монета, электронная ценная бумага, и др.), а также порядок сбора документа из неупорядоченного набора атомарных данных и использования для доступа к ним атомарных программных модулей; шаблон в терминах теории защиты информации является формальной политикой безопасности в работе с данным электронным документом, портативным интеллектуальным носителем информации, а в терминах криптографии – формальным правилом применения криптосистемы;

• универсальной программы-среды, которая интерпретирует *XML*-документы (парсер *XML*-документов) и выполняет атомарные программные модули (подобно виртуальной *Java*-машине);

• программных интерфейсов работы с физическими устройствами–носителями атомарных данных (например, *PKCS*#11 – с интеллектуальными картами, *USB*-токенами, драйверами и программами работы с нетбуками и карманными компьютерами).

Прикладная программа обработки данных работает только с функциями программного интерфейса высокого уровня, например *Microsoft CRYPTOAPI* и не изменяется даже при изменении формы представления данных, при новых требованиях к их защите и даже при изменении формы документа или перечня обрабатываемых документов.

«Ключом», алгоритмом сбора и алгоритмом доступа к электронному документу есть *XML*-документ, содержащий описание данных электронного документа и программы (ссылка на программы) обработки этих данных. Таким образом, электронный документ «собирается» только в необходимый момент времени; при добавлении/модификации отдельных полей электронного документа изменяются только *XML*-шаблон и добавляются недостающие атомарные данные или атомарные программные модули.

Универсальная программная среда (например виртуальная *Java*-машина с *XML*-парсером) интерпретирует *XML*-документ и выполняет атомарные программные модули в соответствии с выбранной политикой безопасности. Так, образуется единая реализация работы с ценными данными для любой программно-аппаратной платформы – единая реализация для ПЭВМ, карманных компьютеров, интеллектуальных карт, *USB*-токенов и пр.

Данный подход позволяет применять достаточно простую формальную модель описания для обеспечения *гарантированного доказательства уровня безопасности.*

Так, любое средство защиты информации представляется как суперпозиция «атомарных» множеств:

F – множество «примитивных» (атомарных) механизмов защиты, примером такого механизма может быть реализация отдельного криптографического примитива с помощью *Java*-технологии (*Java-applet*);

M – множество неупорядоченых данных, подлежащих защите; при этом множество M допополнительно разбивается на подмножества $M = \bigcup_{i=1}^{n} M_i$; каждое сообщение – это подмножество $\dot{M} \subseteq M$, $\dot{M} = \bigcup_{i=1}^{k} M_i$, $k < n$, при этом, как правило, образование сообщения без знания «порядка» (или шаблона) – сложная вычислительная задача;

S, P – множества «шаблонов» и «операций» над множествами M и $S \times F$ соответственно (каждый элемент множества S однозначно определяет подмножество $\dot{M}$). Практической реализацией множества S может служить *XML*-структура, использующая специальный язык описания цифровых защищенных носителей информации – *Ukraine security language* (*USL*). Во введенной модели элементы S можно рассматривать как ключ, определяющий подмножество $\dot{M}$, т.е. отношение эквивалетности на множестве M.

Криптографический протокол описывается как упорядоченный вектор множества P. Элементы множества P задают отображение $S \times F \to 2^M$, а протоколы – векторное простран-

ство над множеством P, здесь 2^M – множество всех подмножеств множества M.

Заметим, что при таком описании корректно представляется известный факт зависимости стойкости системы КЗИ не только от правильной реализации и применения ее механизмов, но и от характеристик открытого текста, который описывается множеством S. При этом выбирается способ разбиения множества M как решение задачи оптимизации по отношению максимизации критерия формальной стойкости системы при ограничении эффективности обработки данных. Свойства отображений $S \times F \to 2^M$ как криптографических преобразований рассмотрены в работе [17].

1. *Таненбаум Э.*, *Ван Стен М.* Распределенные системы. Принципы и парадигмы. – СПб.: Питер, 2003. – 877 с.
2. *Лозовюк А.* Заоблачные вычисления / Хакер. Ж. от компьютерных хулиганов. – 2009. – № 5. – С. 22–25.
3. *Сухорослов О.В.* Новые технологии распределенного хранения и обработки больших массивов данных. – *www.sci-innov.ru*
4. *Самойленко А.* Виртуализация: новый подход к построению *IT*-инфраструктуры. – *www.ixbt.com*
5. *Богуш В.М.*, *Довидьков О.А.*, *Кудін А.М.* Перспективи розвитку автоматизованих систем обробки конфіденційної інформації загального призначення // Вісн. Держ. ун-ту інформаційно-комунікаційних технологій. – 2003. – **1**. – № 1. – С. 42–46.
6. *Комп'ютерні* технології криптографічного захисту інформації на спеціальних цифрових носіях: Навч. посібник. / В.К. Задірака, А.М. Кудін, В.О. Людвиченко та ін. – Київ–Тернопіль: Підручники та посібники, 2007. – 272 с.
7. *Специальные* цифровые носители информации – теория, технология, применение / В.К. Задирака, А.М. Кудин, В.А. Людвиченко и др. // Искусственный интеллект. – 2008. – № 3. – С. 631–638.
8. *Cloud* Security Is Not (Just) Virtualization Security / M. Christodorescu, R. Sailer, D. Lee Schales et al. // CCSW'09, Nov. 13, 2009. – P. 97–102.
9. *Топорков В.В.* Модели распределенных вычислений. – М.: ФИЗМАТЛИТ, 2004. – 320 с.
10. *Вимоги* до форматів даних електронного документообігу в органах виконавчої влади / Затверджено наказом Державного комітету інформатизації України від 14.08.2009 № 49.
11. *Грайворонський М.В.*, *Новіков О.М.* Безпека інформаційно-комунікаційних систем. – К.: Вид. гр. BHV, 2009. – 608 с.
12. *Пономарев В.Л.* НЕТБУК: выбор, эксплуатация, модернизация. – СПб.: БХВ-Петербург, 2009. – 432 с.
13. *Пластиковые* карты / Л.В. Быстров, А.С. Воронин, А.Ю. Гамольский и др. – М.: БДЦ-пресс, 2005. – 624 с.
14. *Бабенко Л.К.*, *Ищуков С.С.*, *Макаревич О.Б.* Защита информации с использованием смарт-карт и электронных брелоков. – М.: Гелиос АРВ, 2003. – 352 с.
15. *Каминская Л.* Электронная бумага: из мира научной фантастики – в реальность. – *http://itc.ua*
16. *Щербаков Л.Ю.*, *Домашев А.В.* Прикладная криптография. Использование и синтез криптографических интерфейсов. — М.: Русская Редакция, 2003. – 416 с.
17. *Кудин А.М.* Об одном классе криптографических преобразований для модели источников информации Колмогорова / Пр. міжнар. симп. «Питання оптимізації обчислень (ПОО–XXXV)», присвяченого 40-річчю І Симп. та літньої матем. шк. з питань точності й ефективності обчислювальних алгоритмів, Київ–Одеса, 1969 р. – К.: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2009. – Т. 1. – С. 394–399.

Поступила 21.05.2010

Тел. для справок: (044) 526-0288 (Киев)
E-mail: *zvk*140*@ukr.net*