ИНФОРМАТИКА

2005 октябрь-декабрь № 4

УДК 681.324.067

Е.А. Цынкевич

ОПРЕДЕЛЕНИЕ КРИТЕРИЕВ ПРАВОМОЧНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Рассматривается проблема оценки защищенности систем электронного документооборота, включая определение понятия правомочности электронного документа, предложены основные критерии оценки правомочности электронного документа в соответствии с существующими в Республике Беларусь нормативно-правовыми актами. Рассмотрены задачи определения критериев, используемых для оценки правомочности электронных документов в системах электронного документооборота различного назначения.

Введение

Массовое производство и эксплуатация информационных систем и сетей самых разнообразных масштабов и назначений придали особую актуальность проблеме подтверждения подлинности и достоверности передаваемой в них информации. Наиболее эффективным решением данной проблемы признано использование электронных документов (ЭД) в виде передаваемой информации, заверенной с помощью электронной цифровой подписи (ЭЦП). Уже в ближайшем десятилетии более 90 % от общего числа передаваемых в электронном виде сообщений будут составлять ЭД, связанные с финансовым обслуживанием экономических процессов, электронной торговлей, банковской деятельностью и т. д. Эти и целый ряд других направлений, которые были определены в Окинавской Хартии глобального информационного общества, принятой 22 июля 2000 г. странами «восьмерки», должны развивать национальные информационные инфраструктуры, совместимые между собой на основе унификации требований к процессам формирования и обработки циркулирующих в них ЭД [1].

В реально действующих автоматизированных системах электронного документооборота ЭД рассматривается как объект, содержащий информацию, на основании которой в системе должны быть выполнены определенные действия. Исполнение ошибочных либо специально сформированных злоумышленниками ЭД может нанести пользователям этих систем ощутимый ущерб. В связи с этим перед началом реализации операций, предписываемых полученным ЭД, необходимо проверить выполнение множества установленных в системе требований, при нарушении которых ЭД не может быть принят к исполнению, т. е. решить задачу по оценке правомочности ЭД в понятиях конкретной системы. Для этого необходимо выявить с учетом действующих в данной области нормативно-правовых и технических нормативно-правовых актов множество предъявляемых требований, а также разработать формальные модели и методы оценки их выполнения. Использование нормативных требований обеспечит придание правового статуса принимаемым решениям, а создание формальных моделей и методов позволит осуществить программно-аппаратную поддержку принятых решений. Выполнение поставленной задачи по оценке правомочности ЭД в конкретной системе электронного документооборота должно осуществляться в рамках проведения комплекса мероприятий по обеспечению безопасности этой системы в соответствии с ее профилем защиты [2].

1. Анализ состояния и существующие проблемы определения правомочности электронного документа

Сегодня в Республике Беларусь существует техническая нормативно-правовая база, необходимая для решения задач по установлению правомочности в части обеспечения подлинности и целостности ЭД в соответствии с требованиями Закона «Об электронном документе» [3].

Выполнение этих требований реализуется на основе использования методов криптографической защиты [4], которые с достаточной степенью достоверности обеспечивают проверку следующих утверждений: «ЭД подписан с помощью личного ключа, соответствующего ис-

пользуемому для проверки открытому ключу» и «после установки ЭЦП в ЭД не были внесены изменения». Однако для большинства реально функционирующих систем электронного документооборота эта проверка является необходимым, но не достаточным условием подтверждения правомочности ЭД, так как в них существует множество дополнительных требований по установлению правомочности, выполнение которых не может быть подтверждено лишь проверкой данных утверждений.

В соответствии с предложенной в работе [5] классификацией критичных информационных объектов системы электронного документооборота могут быть отнесены к классам А1–А3, т. е. к системам с наиболее высоким уровнем защищенности охраняемого информационного ресурса, компрометация которого приводит к срыву выполнения данными системами их функций (задач). Здесь же констатируется, что для решения проблемы обеспечения информационной безопасности в критичных информационных объектах необходимо учитывать новые для отечественной практики дополнительные требования.

В наиболее распространенных автоматизированных системах электронного документооборота наличие дополнительных требований является следствием того, что в них циркулируют ЭД, отличающиеся своим назначением, статусом, составом и форматами реквизитов, временными условиями и причинно-следственными связями их формирования, передачи, обработки и хранения. Исходя из отличий, носящих принципиальный характер, множество ЭД разбивается на классы. Пользователи данных систем также имеют принципиальные отличия, с учетом которых ЭД, относящиеся к различным классам, формируются различными группами пользователей в соответствии с ролью этих пользователей, служебными обязанностями и предоставленными им полномочиями. Нарушение перечисленных условий должно рассматриваться как нарушение правомочности ЭД, оказывающее существенное влияние на безопасность системы в целом. Следовательно, предпринимаемые действия по их устранению должны реализовываться в рамках комплекса мероприятий, проводимых по обеспечению безопасности всей системы.

В данной статье формирование пользователями систем ЭД рассматривается как процесс, состоящий из последовательности установленных в системе технологических процедур, каждая из которых завершается выработкой ЭЦП лица, ответственного за ее выполнение. К множеству данных процедур относятся процедуры по заполнению и контролю содержимого ЭД, а также процедуры по его предварительному использованию.

2. Формальная модель механизмов, обеспечивающих подтверждение правомочности электронных документов в автоматизированных системах электронного документооборота

Целесообразно рассмотреть пример формальной модели механизмов, обеспечивающих подтверждение правомочности ЭД в автоматизированных системах электронного документооборота. Основными структурными элементами предлагаемой модели являются множества:

$P = \{ p_g \}$ – групп пользователей;

$H = \{ h_g \}$ – требований к атрибутам пользователей и их значениям или совокупностям атрибутов пользователей и их значениям, участвующим в процедуре отнесения конкретного пользователя к соответствующей группе;

$O = \{ o_i \}$ – операций, проводимых в процессе формирования ЭД;

$E = \{ e_k \}$ – классов ЭД;

$A = \{ a_k \}$ – требований к атрибутам ЭД и их значениям или совокупностям атрибутов ЭД и их значениям, участвующим в процедуре отнесения конкретного ЭД к соответствующему классу.

Использование одинаковых индексов в предложенной системе обозначений структурных элементов обусловлено наличием причинно-следственных связей между элементами множеств P и H и множеств E и A. Кроме того, необходимо отметить, что под требованиями к атрибутам и их значениям или совокупностям атрибутов и их значениям подразумеваются формализованные спецификации требований, устанавливающие факт наличия у объекта определенных атрибутов и принадлежности их значений к определенным множествам значений с последующим вынесением вердикта о соответствии конкретного объекта конкретной спецификации требований. При разработке данных спецификаций рекомендуется использовать

абстрактно-синтаксические нотации, функции из семейства булевых функций, аппарат вычисления предикатов. Очевидно, что первичными являются множества H и A, элементы которых и определяют соответствующие им элементы множеств P и E. Таким образом, вначале необходимо определить множества H и A, что позволит в дальнейшем однозначно относить конкретного пользователя или конкретный ЭД к соответствующей группе пользователей p_g или классу ЭД e_k, руководствуясь следующими правилами:

1. Пользователь p включается в состав группы пользователей p_j, входящей в состав множества P, тогда и только тогда, когда на основании соответствующих ему атрибутов и их значений выносится вердикт о соответствии атрибутов данного пользователя элементу h_j, входящему в состав множества H.

2. ЭД e включается в класс ЭД e_n, входящий в состав множества E, тогда и только тогда, когда на основании соответствующих ему атрибутов и их значений выносится вердикт о соответствии атрибутов данного документа элементу a_n, входящему в состав множества A.

После определения множеств P, O и E в предлагаемой модели вводится понятие области правомочности ЭД как декартового произведения множеств $D = P, O, E$. В области правомочности ЭД должны быть определены подобласти, подтверждающие правомочность ЭД для любого входящего в них трехмерного кортежа $g = (p,o,e)$, где $p \in P$, $o \in O$, $e \in E$. ЭД признается правомочным только в том случае, если соответствующий ему кортеж попадает в подобласть, подтверждающую его правомочность.

Использование предлагаемой модели призвано решить задачу установления правомочности ЭД с учетом ролей конкретных пользователей в автоматизированной системе электронного документооборота, полномочий этих пользователей на выполнение определенного для каждого из них множества операций в процессе формирования определенных классов ЭД, требований к составу и содержанию атрибутов ЭД в зависимости от их принадлежности к определенному классу ЭД.

3. Угрозы, возникающие в процессе электронного документооборота

Проверка правомочности ЭД направлена на парирование угроз, возникающих в процессе электронного документооборота, поэтому при построении формальной модели механизмов, обеспечивающих подтверждение правомочности ЭД в конкретных автоматизированных системах электронного документооборота, необходимо учитывать угрозы, которые возникают в процессе электронного документооборота.

К общим угрозам, которые характерны для всех систем электронного документооборота и приводят к нарушению правомочности циркулирующих в них ЭД, можно отнести следующие:

– передачу ЭД от несанкционированных пользователей;

– попытку выполнения авторизованным пользователем при формировании и передаче ЭД определенных действий без соответствующих прав на их выполнение;

– отказ пользователя от сформированного и переданного им документа;

– нарушение целостности ЭД в процессе их передачи (хранения);

– нарушение синтаксических и семантических требований (правил) формирования ЭД;

– нарушение регламентных требований (правил) при формировании и передаче ЭД.

С учетом функционального назначения систем электронного документооборота и специфики их эксплуатации данный перечень может уточняться. Наличие реальных угроз для систем электронного документооборота требует обязательного решения задач по обеспечению их безопасности.

4. Критерии правомочности электронного документа

Во введении к данной статье было сказано, что оценка правомочности ЭД в конкретной системе электронного документооборота должна осуществляться в рамках проведения комплекса мероприятий по обеспечению безопасности этой системы в соответствии с ее профилем защиты. Возможность использования данного утверждения связана с принятием в 1999 г. международного стандарта «ISO/IES 15408: 1999. Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий», который более извес-

тен под названием «Общие критерии». В Республике Беларусь Общие критерии приняты в качестве государственного стандарта [6].

С учетом применения подходов, изложенных в Общих критериях, в качестве объекта оценки предлагается рассматривать автоматизированные системы электронного документооборота с циркулирующими в них ЭД. Таким образом можно использовать методологию Общих критериев для решения задачи обеспечения правомочности ЭД в системах электронного документооборота в рамках реализации соответствующего профиля защиты.

Критериями правомочности предлагается считать соответствие ЭД требованиям:

– Закона «Об электронном документе»;

– действующих технических нормативно-правовых актов;

– отражающим специфику автоматизированных систем электронного документооборота.

Разработка данных критериев должна быть направлена на уменьшение рисков, связанных с использованием электронного документооборота, и должна включать решение следующих задач:

– определение множества угроз, возникающих в процессе электронного документооборота;

– анализ влияния угроз, возникающих в процессе электронного документооборота, на правомочность ЭД;

– определение множества требований, выполнение которых обеспечивает подтверждение правомочности ЭД.

Для признания ЭД правомочным необходимо убедиться, что в процессе его формирования, преобразований, передачи и хранения были выполнены все требования к взаимодействию посредством ЭД, установленные в конкретной автоматизированной системе.

Критерии установления правомочности любого документа, в том числе и электронного, основываются на проверке выполнения определенного множества требований, предъявляемых к документам данного класса в процессе их жизненного цикла.

К перечню таких требований относятся в первую очередь требования, предъявляемые к любым документам независимо от сферы их применения. Так, ЭД, используемые в соответствии с работой [7] во взаимодействиях типа «Субъект – Субъект (С – С)», «Субъект – Объект (С – О)» и «Объект – Субъект (О – С)», в обязательном порядке должны удовлетворять требованиям Закона «Об электронном документе» [3]:

– ЭД не может применяться в случаях наличия ограничений на применение ЭД, предусмотренных законодательством Республики Беларусь (ст. 2);

– ЭД не может пересылаться с помощью средств связи в случаях, когда это противоречит законодательству Республики Беларусь и международным договорам Республики Беларусь (ст. 2);

– ЭД должен создаваться, обрабатываться, передаваться, храниться и защищаться с помощью программных и технических средств, подлежащих сертификации в порядке, установленном законодательством Республики Беларусь (ст. 6, 21);

– ЭД должен иметь структуру, установленную Законом «Об электронном документе», содержать реквизиты, позволяющие ее идентифицировать, и быть представленным в форме, понятной для восприятия человеком (ст. 6, 7);

– все экземпляры ЭД, зафиксированные на машинном носителе и идентичные один другому, должны использоваться как оригиналы, приравниваться к документу на бумажном носителе и иметь одинаковую с ним юридическую силу (ст. 9, 11);

– ЭД подлежат в установленном порядке государственной регистрации в случаях, если это требуется законодательством Республики Беларусь (ст. 11);

– должна обеспечиваться идентичность используемого пользователем открытого ключа проверки подписи тому ключу, который зафиксирован в карточке открытого ключа проверки подписи (ст. 14);

– индивидуальные предприниматели и юридические лица, осуществляющие оказание услуг по распространению в установленном законом порядке открытых ключей проверки подписи, должны иметь лицензию на оказание услуг по распространению открытых ключей проверки подписи (ст. 15);

– хранение ЭД должно производиться организациями, осуществляющими архивную деятельность и деятельность по хранению документированной информации. Порядок, условия и особенности хранения ЭД определяются законодательством Республики Беларусь (ст. 16).

В дополнение к законодательным требованиям, предъявляемым к любым электронным документам независимо от сферы их применения, относятся и требования, установленные в основополагающих стандартах. Так, в качестве государственного стандарта Республики Беларусь был принят СТБ 1221-2000 «Документы электронные. Правила выполнения, обращения и хранения» [8]. Согласно этому документу:

– объектами защиты ЭД являются их обязательные реквизиты и ЭЦП;

– изменения в ЭД могут вноситься только на стадиях создания и оперативного обращения;

– при любых изменениях ЭД, которые заверяются ЭЦП, изменяемые ЭД аннулируют;

– изменения в ЭД вносятся подразделениями организаций, отвечающими за разработку или сопровождение информационных систем, в среде которых создаются ЭД;

– для хранения ЭД с постоянным сроком хранения должны использоваться форматы файлов, согласованные с государственным архивом.

Все предъявляемые к ЭД требования должны быть учтены при определении критериев установления правомочности ЭД в процессе их использования в автоматизированных системах. Поэтому помимо требований Закона «Об электронном документе» и СТБ 1221-2000 необходимо учитывать также и дополнительные требования, отражающие специфику автоматизированных систем электронного документооборота, которым должна соответствовать поступившая в автоматизированную систему информация для ее идентификации как ЭД и установления ее правомочности.

С учетом назначения систем электронного документооборота и их функциональных особенностей предлагается в состав дополнительных процедур проверки выполнения требований, соответствие которым также является необходимым условием подтверждения правомочности ЭД, включить процедуры, проверяющие выполнение следующих требований:

– синтаксических и семантических, предъявляемых к формируемым документам (например, к составу и форматам реквизитов и правилам их заполнения);

– отражающих полномочия пользователей относительно формируемых ими ЭД (например, политики использования ключей ЭЦП);

– отражающих регламент для выявления аномального поведения пользователей системы;

– к системам управления криптографическими ключами пользователей;

– к распознаванию, записи, хранению и анализу информации о деятельности, связанной с обработкой поступивших в систему ЭД;

– к защите данных пользователей (например, защите конфиденциальности данных о полномочиях пользователя в системе, обеспечению целостности хранимых открытых ключей пользователей).

В самом общем случае множество функциональных требований безопасности, выполнение которых обеспечивает подтверждение правомочности ЭД в системах электронного документооборота и которые включаются в профили защиты систем данного класса, может быть представлено в следующем виде.

По классу *FAU «Аудит безопасности»* – должна существовать обработка всех нарушений, обнаруженных в процессе выполнения проверок по подтверждению правомочности ЭД, в том числе:

– правил формирования ЭД (ЭД подписан на неизвестном ключе, неизвестен формат ЭД и т. п.);

– целостности полученных ЭД;

– требований регламента передачи ЭД (например, несоблюдение отведенных временных интервалов для передачи ЭД определенного типа; превышение максимального количества ЭД определенного типа, передаваемых за один временной интервал; повторная посылка уже обработанного ЭД и т. п.);

– требований использования открытых ключей пользователей (например, в случаях изменения состояния ключей пользователей необходимо должным образом реагировать на ЭД, поступившие от данных пользователей);

– требований политик использования ключей пользователя (например, если пользователь не уполномочен подписывать документы данного типа).

По классу *FCO «Связь»* – для того чтобы избежать угроз отказа пользователей системы от факта отправки электронного документа либо его получения, необходимо обеспечить механизмы подтверждений фактов приема и передачи информации.

По классу *FCS «Криптографическая поддержка»* – для избежания угроз компрометации личного ключа пользователя, а также для обеспечения достоверности информации об открытом ключе и его состоянии для проверки ЭЦП конкретного ЭД необходимо обеспечить:

– сервисы своевременного управления состоянием ключей подписи в связи с возможностью изменения состояния ключей пользователей на протяжении их жизненного цикла;

– целостность открытых ключей пользователей, а также сервисы верификации этих открытых ключей;

– надежность распределения открытых ключей;

– доступ к открытым ключам пользователей;

– конфиденциальность личного ключа пользователя при его генерации и хранении на ключевом носителе.

По классу *FDP «Защита данных пользователя»* – для того чтобы все пользователи системы электронного документооборота могли воспользоваться достоверной информацией о текущем состоянии ключей других пользователей и их полномочиях, а также иметь возможность получить эти ключи, должна быть обеспечена защита:

– личных данных пользователя (о его роли в системе, полномочиях и т. п.);

– целостности открытого ключа пользователя;

– данных о состоянии ключей пользователей.

По классу *FIA «Идентификация и аутентификация»* – для того чтобы установить, может ли быть признан подлинным конкретный ЭД, исходя из имеющейся информации о владельце личного ключа, на котором выработана ЭЦП данного документа, должны обеспечиваться однозначные идентификация и аутентификация авторизованных пользователей, а также назначение им атрибутов безопасности.

По классу *FRU «Использование ресурсов»* – для того чтобы все пользователи системы электронного документооборота могли воспользоваться информацией о текущем состоянии ключей других пользователей, их полномочиях, а также иметь возможность получить эти ключи, должен быть обеспечен гарантированный доступ всех субъектов, имеющих на это необходимые полномочия, к открытым ключам пользователей системы, а также к информации об их состоянии.

По классу *FTA «Доступ к объекту оценки»* – для обеспечения защиты от угроз превышения авторизованным пользователем предоставленных ему полномочий при формировании и передаче ЭД, а также от угроз передачи ЭД от неавторизованных пользователей ЭД пользователей должны обрабатываться на основании заранее определенной роли этого пользователя в системе. Любое аномальное поведение пользователей должно обнаруживаться и протоколироваться.

По классу *FTP «Доверенный путь/канал передачи данных»* – должна быть обеспечена конфиденциальность и/или целостность передаваемой информации с помощью использования доверенного канала при передаче информации, касающейся личных данных пользователей, либо информации об изменении состояния их ключей подписи.

Заключение

Анализ существующей нормативной базы по обеспечению защищенности объектов информационных технологий показал, что непосредственное использование совокупности рассмотренных выше требований нормативно-правовых актов не является достаточно полной базой для создания системы оценки защищенности систем электронного документооборота от использования в них неправомочных документов. В связи с этим возникла необходимость в разработке формальных подходов к оценке защищенности систем электронного документооборота, основанных на построении моделей, учитывающих требования действующих в Республике Беларусь законодательных, нормативно-правовых и технических нормативно-правовых актов, а также специфические особенности применения систем данного класса. Построение фор-

мальных моделей подтверждения правомочности ЭД в автоматизированных системах электронного документооборота и разработка программно-технических средств и организационных мероприятий, обеспечивающих их практическую реализацию, предлагается осуществлять на основе определения в составе соответствующего профиля защиты критериев оценки правомочности ЭД, которые гарантируют в данных системах приемлемый уровень выполнения требований по подтверждению правомочности циркулирующих в них ЭД.

Список литературы

1. Полещук М.И. Обеспечение гарантии безопасности объектов информационных технологий на методологической основе Общих критериев // Управление защитой информации. – Т. 9. – № 3. – 2005. – С. 284–292.

2. Цынкевич Е.А. Критерии правомочности электронных документов: мат. IX Междунар. конф. «Комплексная защита информации». – Мн., 2005. – С. 106–107.

3. Об электронном документе: Закон Республики Беларусь от 10 января 2000 г. № 357-З // Национальный реестр правовых актов Республики Беларусь. – 21 января 2000 г. – № 7.

4. СТБ 1176.2-99. Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи.

5. Крюкова Э.П., Томина Г.Д. К вопросу о классификации критичных информационных объектов // Управление защитой информации. – Т. 6. – № 4. – 2002. – С. 403–406.

6. СТБ 34.101.1-3. Критерии оценки безопасности информационных технологий.

7. Конявский В.А., Гадасин В.А. Основы понимания феномена электронного документооборота. – Мн.: Беллитфонд, 2004.

8. СТБ 1221-2000. Документы электронные. Правила выполнения, обращения и хранения.

Поступила 19.09.05

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: gregoir@tut.by

E.A. Tsynkevich

CRITERIA OF THE ELECTRONIC DOCUMENTS COMPETENCE

A problem of information security analysis of electronic document interaction systems and a notion of the electronic document competence are considered, the basic criteria of the electronic document competence are defined. An approach to the definition of electronic document competence criteria for electronic document interaction systems designed for different purposes is proposed.