УДК 004.9; 004.056:061.68

Е.А. Цынкевич

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРАВОМОЧНОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Рассматривается проблема обеспечения правомочности электронных документов, формируемых и применяемых в системах электронного документооборота, и в качестве подхода к ее решению предлагается использование математической модели правомочности. Исходя из общего определения понятия правомочности электронного документа формально определяется множество элементов моделируемой системы, множество ее состояний, удовлетворяющих условию и свойству правомочности, а также правил перехода, обеспечивающих правомочность системы и циркулирующих в ней документов.

Введение

Бурное развитие информационных систем и сетей, обеспечивающих обмен и обработку циркулирующих в них данных самого разнообразного назначения, обусловило особую актуальность проблемы подтверждения их подлинности и достоверности, т. е. придания им официального статуса и юридической значимости. Наиболее эффективным решением данной проблемы признано использование электронных документов (ЭД) в виде передаваемой информации, заверенной с помощью электронной цифровой подписи (ЭЦП). Прогнозируется, что в ближайшем десятилетии более 90 % от общего числа передаваемых в электронном виде сообщений будут составлять ЭД, связанные с финансовым обслуживанием процессов промышленной и экономической деятельности, электронной торговлей, банковской деятельностью и т. д. Кроме свойств, обеспечивающих функциональную полезность данных систем и их информационную совместимость, эти системы должны обладать и свойствами, обеспечивающими правомочность циркулирующих в них ЭД [1].

В самом общем виде ЭД определяется как информация, зафиксированная на машинном носителе и соответствующая требованиям, установленным Законом «Об электронном документе» [2]. В процессе создания и функционирования конкретной системы электронного документооборота (далее – система) ЭД рассматриваются как объекты, содержащие информацию, на основании которой в системе выполняются определенные действия. Исполнение ошибочных либо специально сформированных злоумышленниками ЭД может нанести пользователям этих систем ощутимый ущерб. Поэтому формирование и обработка ЭД должны осуществляться с соблюдением определенного в системе множества требований, при нарушении которых ЭД не может быть сформирован или принят к исполнению, т. е. решить проблему обеспечения правомочности ЭД в понятиях конкретной системы.

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» [2]. Выполнение этих требований реализуется на основе использования методов криптографической защиты [3], которые с достаточной степенью достоверности обеспечивают проверку следующих утверждений: «*ЭД подписан с помощью личного ключа, соответствующего используемому 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 [1].

При создании систем, обеспечивающих правомочность циркулирующих в них ЭД, на основе традиционных методов в качестве доказательной базы того, что созданная в соответствии с проектной документацией система обладает прогнозируемыми свойствами, как

правило, используются протоколы и акты тестовых прогонов и приемосдаточных испытаний. Получаемые в итоге результаты носят вероятностный характер и требуют больших затрат даже для получения достаточно грубых оценок по практической пригодности сравнительно простых систем, при этом наблюдается экспоненциальная зависимость затрат от сложности систем и достоверности получаемых результатов. В связи с этим является весьма актуальным применение в процессе решения указанной проблемы более рациональных методов.

Цель данной работы – показать возможности использования при решении проблемы обеспечения правомочности ЭД методов математического моделирования, представленных в работе [4] и известных в научной литературе как модель Белла-Лападула.

Уже на этапе проектирования системы данные методы дают возможность анализировать ее свойства с получением строгих доказательств их наличия или отсутствия. Применение математических методов анализа позволяет во многих случаях получать абсолютные, а не вероятностные оценки создаваемой системы с заменой экспоненциальной зависимости затрат на пропорциональную зависимость.

1. Математическая модель правомочности электронных документов и задачи, решаемые в процессе ее разработки

В данном случае под математической моделью подразумевается совокупность понятий, которые соответствуют элементам моделируемой системы, и формальных определений этих элементов, обеспечивающих возможность их однозначного толкования и идентификации с применением соответствующих обозначений в виде математических символов и выражений, отражающих взаимосвязи элементов моделируемой системы, правила взаимодействия и накладываемые ограничения в процессе математического моделирования.

В отличие от классического использования математической модели для приближенного описания какого-либо класса явлений внешнего мира, выраженного с помощью математической символики, построение математической модели правомочности ЭД, как правило, совмещается с процессом разработки самой системы электронного документооборота, что не требует в дальнейшем проведения доказательств их адекватности.

Разработка математической модели правомочности ЭД сводится к решению следующих задач:

– определению понятия правомочности ЭД и набора требований, которые в обязательном порядке должны соблюдаться в процессе функционирования системы, включая при необходимости и требования по обеспечению их юридической значимости;

– конкретизации понятий, используемых при определении набора вышеупомянутых требований, через формальные определения и обозначения элементов, входящих в состав моделируемой системы, и их взаимосвязей в процессе функционирования системы;

– определению набора правил перехода и доказательству, что система, удовлетворяющая установленному набору требований и функционирующая по установленным правилам, обеспечивает правомочность ЭД в соответствии с принятым для данной системы определением правомочности.

С учетом того что основные проблемы, связанные с решением рассматриваемых задач, разделяются на две группы: общие и специфические, при изложении последующих разделов статьи, содержащих практические рекомендации, основное внимание уделено решению общих проблем, а подходы к решению специфических проблем демонстрируются лишь на отдельных примерах.

2. Определение правомочности электронных документов

Под правомочностью ЭД в данной статье подразумевается совокупность установленных в секторе действенности ЭД (системе) свойств, позволяющих ему оказывать определенное воздействие на этот сектор (систему) [5]. Таким образом, правомочность ЭД, впрочем, как и сами

ЭД, относится к понятиям, определяемым в процессе создания и функционирования конкретной системы.

В наиболее распространенных системах используются 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 и используются разными группами пользователей в соответствии с ролью этих пользователей, служебными обязанностями и предоставленными им полномочиями [6]. Нарушение перечисленных условий должно рассматриваться как нарушение правомочности ЭД, оказывающее существенное влияние на безопасность системы в целом, и, следовательно, предпринимаемые действия по их устранению должны реализовываться в рамках комплекса мероприятий, проводимых по обеспечению безопасности всей системы.

ЭД является правомочным, если в процессе его формирования и использования были выполнены в полном объеме все требования по обеспечению правомочности.

Для более строгого определения данного понятия сформулируем основные требования, которые должны соблюдаться в системах в процессе формирования и использования ЭД:

– формирование и использование в системе ЭД должно осуществляться в виде установленных последовательностей действий, выполняемых по определенным правилам, учитывающим состояние, в котором находится система в момент их выполнения;

– начальное и каждое последующее (текущее) состояние системы должно удовлетворять условию и свойству правомочности данной системы;

– каждое выполняемое по определенным в системе правилам действие должно переводить систему в состояние, также удовлетворяющее условию и свойству правомочности данной системы.

С учетом этого правомочность ЭД можно определить следующим образом: ЭД является правомочным, если все действия, выполняемые в процессе его формирования и использования, проводились в строгом соответствии с перечисленными выше основными требованиями.

Далее следует отметить, что для каждого ЭД на момент его исполнения должны иметься определенные системой гарантии соблюдения установленных требований по обеспечению его правомочности на предшествующих этапах. Одной из таких гарантий может являться наличие ЭЦП полномочного лица, отвечающего за выполнение данных требований в процессе формирования ЭД, другой – то, что все действия по формированию и обеспечению правомочности ЭД осуществлялись без выхода за пределы зоны безопасности [7]. С учетом того что любое нарушение в процессе формирования или контроля ЭД требований безопасности должно рассматриваться как нарушение требований, обеспечивающих его правомочность, эти понятия разделяться не будут.

Объем проводимых работ в процессе контроля правомочности ЭД, выполняемых в конкретном узле системы, зависит от класса, к которому относится контролируемый ЭД, доступной в данном узле нормативно-справочной информации (НСИ) и полномочий субъектов, обеспечивающих их проведение.

Требования по обеспечению правомочности должны выполняться на всех стадиях жизненного цикла ЭД, включая их создание, пересылку, обработку, хранение и уничтожение.

3. Определения и обозначения элементов, входящих в состав моделируемой системы

Начнем с формального определения элементов моделируемой системы, соответствующих ее терминальным или агрегированным компонентам, которые, в свою очередь, делятся на объекты и субъекты.

Вначале рассмотрим вопрос формального определения одного из основных объектов системы – ЭД, которое должно соответствовать статье 7 Закона «Об электронном документе» [2], устанавливающей следующее:

– ЭД состоит из двух неотъемлемых частей – общей и особенной;

– общая часть ЭД состоит из информации, составляющей содержание документа, информация об адресате относится к общей части;

– особенная часть ЭД состоит из одной или нескольких ЭЦП.

Кроме того, положения статьи 6 устанавливают, что ЭД должен:

– создаваться, обрабатываться, передаваться и храниться с помощью программных и технических средств;

– иметь структуру, установленную настоящим Законом, и содержать реквизиты, позволяющие ее идентифицировать.

Отметим, что приведенные положения не определяют:

– какова очередность размещения данных, относящихся к общей и особенной частям ЭД;

– относятся ли реквизиты, позволяющие идентифицировать структуру ЭД, к его содержанию и, следовательно, к его общей части;

– может ли общая часть одного ЭД содержать другие ЭД и т. д.

Ответы на поставленные выше вопросы могут быть получены лишь при наличии в каждой конкретной системе формального описания структур используемых в ней ЭД, что позволит в дальнейшем однозначно трактовать все действия, связанные с обеспечением правомочности ЭД в процессе их формирования и использования.

Для упрощения дальнейшего изложения предлагается в качестве формального метаязыка при определении множества объектов PO и требований к структурам рассматриваемых ЭД использовать форму Бэкуса – Наура (БНФ), которая стала популярной после ее применения для описания синтаксиса Алгола-60 [8].

С использованием БНФ-нотаций на верхнем уровне представления структура ЭД в самом общем виде может определяться следующим образом:

$$
\begin{aligned}
&< O_{ЭД} > ::= < O_{общая\_часть} > < O_{ЭЦП} > | \\
&\qquad < O_{ЭД} > < O_{ЭЦП} >; \\
&< O_{общая\_часть} > ::= < O_{реквизит\_ЭД} > | \\
&\qquad < O_{общая\_часть} > < O_{реквизит\_ЭД} >; \\
&< O_{реквизит\_ЭД} > ::= < O_{элемент\_данных} > | \\
&\qquad < O_{включаемый\_ЭД} >; \\
&< O_{включаемый\_ЭД} > ::= < O_{ЭД} >.
\end{aligned}
$$

Сразу же отметим, что данное определение содержит ответы на три поставленных выше вопроса. Так, первое правило формирования объекта «электронный документ» однозначно определяет порядок следования в структуре ЭД вначале общей, а затем особенной части, а второе правило формирования объекта «электронный документ» устанавливает, что данный объект может содержать одно или несколько ЭЦП, следующих друг за другом. Первое и второе правила формирования второго объекта «общая часть» устанавливают, что общая часть ЭД может состоять из одного либо из нескольких реквизитов. С учетом второго правила формирования объекта «реквизит ЭД» это позволяет в общую часть одного ЭД включать другие ЭД.

Необходимость придания ЭД юридической значимости в соответствии с предложениями, изложенными в [9], на самом верхнем уровне представления может быть определена как

$$
< O_{юр.\_знач.\_ЭД} > ::= < \hat{I}_{\,\hat{i}\,\acute{a}\grave{u}\,\grave{a}\ddot{y}\_\div\grave{a}\tilde{n}\grave{o}\,\ddot{i}} > < \hat{I}_{\,\acute{o}\ddot{a}\hat{i}\,\tilde{n}\grave{o}\,\hat{i}\,\hat{a}\mathring{a}\eth.\_\div.\_\ddot{i}\,\hat{i}\,\_\tilde{n}\grave{o}\,\grave{a}\acute{i}\,\ddot{a}.\_ETSI\_101\_733} > .
$$

Предлагаемый подход обеспечивает однозначность при определении требований к структурам ЭД и предоставляет возможность использования методов грамматического разбора для проверки их выполнения [10].

Далее необходимо учитывать, что реальная система может иметь много пользователей, действующих одновременно в ее узлах на общей базе данных. Для всех пользователей и данных вводится многоуровневая классификация и категории, связанные с пользователями и дан-

ными. По аналогии с [4] при описании модели предлагается вместо пользователей рассматривать некоторые субъекты, к которым будем относить инициированные пользователями процессы, а также программы в ходе их выполнения.

В узлах моделируемой системы на определенных уровнях представления реализуются следующие основные процессы:

$< PR_F >$ – формирования ЭД;

$< PR_C >$ – контроля правомочности ЭД;

$< PR_W >$ – обработки (использования) ЭД.

Данные процессы реализуются, как правило, в виде определенных последовательностей, состоящих из входящих в них процессов и/или элементарных операций (действий), выполняемых поочередно в рамках общей зоны безопасности и содержащих элементы рекурсии.

В качестве формального метаязыка для определения множества допустимых в узлах системы последовательностей PR перечисленных выше процессов и их дальнейшей конкретизации в рамках предлагаемой модели также будем использовать нотации БНФ. С использованием БНФ-нотаций множество допустимых в конкретном узле системы последовательностей процессов $< PRS >$ на верхнем уровне представления может быть определено следующим образом:

$$
\begin{aligned}
< PRS > \; ::= & < PRS_1 > | \\
& < PRS_2 > ; \\
< PRS_1 > ::= & < PR_F > | \\
& < PR_C > \; | \\
& < PRS_1 > \; < PR_F > | \\
& < PRS_1 > \; < PR_C > |; \\
< PRS_2 > ::= & < PR_C > < PR_W > | \\
& < PRS_2 > < PR_W > | \\
& < PRS_2 > < PR_C > | \\
& < PRS_1 > < PRS_2 > .
\end{aligned}
$$

В данном примере предполагается, что все процессы выполняются без нарушения требований, установленных для обеспечения правомочности циркулирующих в моделируемой системе ЭД.

Очевидно, что в реально действующих системах всегда предусматриваются возможности возникновения ошибочных ситуаций, которые они должны обрабатывать соответствующим образом, поэтому приведенный пример может рассматриваться лишь как демонстрация формального определения множества разрешенных последовательностей выполняемых процессов и не может рассматриваться как фрагмент описания реально моделируемой системы.

В то же время отметим, что определенное в приведенном примере множество $< PRS >$ не включает последовательности, начинающиеся с $< PR_W >$ – процесса обработки (использования) ЭД.

Таким образом, определяется одно из основных требований обеспечения правомочности ЭД в реально действующих системах, предусматривающее обязательное выполнение контроля правомочности ЭД, поступившего в ее узловую точку, до того, как он будет обработан (использован).

Кроме того, следует учитывать, что подобное описание может применяться и в качестве исходных данных для генерации программы, которая выполняет анализ поступающих на вход идентификаторов процессов, определяющих порядок их выполнения, с целью установления принадлежности конкретных процессов к определенному множеству разрешенных последовательностей.

Между объектами в системах устанавливаются функциональные отношения FO. Примером функциональных отношений, которые в обязательном порядке должны быть установлены

в каждой рассматриваемой системе, являются отношения, определяющие соответствие общей части ЭД O_M его ЭЦП O_S по процедуре проверки ЭЦП [3]. С учетом того что при определении указанных соответствий используются данные, содержащиеся в сертификате открытого ключа $\{O_p, O_l, O_q, O_r, O_a, O_y\} \in O_{COK}$ и определяющие значения соответствующих им исходных параметров криптографического алгоритма p, l, q, r, a и открытый ключ проверки подписи y, и, принимая, что $[O_M] = M_X$, где M_X – значение Хэш функции, $[O_S] = S$ и т. д., эти функциональные отношения устанавливаются следующим образом:

$$FO_{i1} : 0 < (S - S \bmod 2^r)/2^r;$$
$$FO_{i2} : (S - S \bmod 2^r)/2^r < 2^{r-1};$$
$$FO_{i3} : 0 < S \bmod 2^r;$$
$$FO_{i4} : S \bmod 2^r < q;$$
$$FO_{i5} : (S - S \bmod 2^r)/2^r = h(M_t),$$

где M_t определяется через M и S в соответствии с [3], а $h(M_t)$ определяется в соответствии с [11].

Второй пример, в отличие от предыдущего, не распространяется на все системы, а относится лишь к тем, в которых ЭД содержат определенное множество однотипных числовых реквизитов $\{O_i\}$, принимающих значения из диапазона (a, b), а также реквизит O_{sum}, содержащий их сумму. В этом случае устанавливаемые функциональные отношения имеют вид

$$FO_{j1} : a < [O_i];$$
$$FO_{j2} : [O_i] < b;$$
$$FO_{j3} : \sum_{i=1}^{m} [O_i] \le [O_{sum}];$$
$$FO_{j4} : [O_{sum}] = \sum_{i=1}^{n} [O_i],$$

где FO_{j3} применяется на промежуточных стадиях формирования ЭД, а FO_{j4} – на завершающей стадии, т. е. когда можно утверждать, что множество реквизитов $\{O_i\}$ и реквизит O_{sum} полностью сформированы.

Как отмечалось ранее, в представленной модели элементы системы делятся на объекты (обозначаемые далее как O) и субъекты (обозначаемые далее как S), которые, за исключением элементов, входящих в состав множеств PO, PR и FO (таблица), совпадают с множеством элементов модели Белла-Лападула.

Предполагается, что читатель знаком с моделью Белла-Лападула, поэтому в данной статье не дается подробного описания всех используемых в ней элементов, а представлены лишь элементы, описание которых существенно не зависит от специфических особенностей конкретных систем. К элементам, зависящим от специфических особенностей конкретных систем, например, относятся элементы f_1, f_2, f_3, f_4, определяющие классификационный вектор.

Таблица

Определение множеств элементов *PO*, *PR* и *FO*

Тип элемента	Элементы	Смысловое содержание
PO	$\{PO_1, PO_2, ..., PO_o\}$, $PO_i = \{(PO_i^j)\}$, где (PO_i^j) – j-е правило формирования $O_i \in O$ $< O_i > ::= < O_{i1}^j >< O_{i2}^j >$, где $O_{i1}^j \in O$ и $O_{i2}^j \in O$	*Формальные описания объектов*: множество бинарных правил формирования нетерминальных объектов через входящие в них объекты
PR	$\{PR_1, PR_2, ..., PR_p\}$, $PR_i = \{(PR_i^j)\}$, где (PR_i^j) – j-е правило формирования $PR_i \in PR$ $< PR_i > ::= < PR_{i1}^j >< PR_{i2}^j >$, где $PR_{i1}^j \in PR$ и $PR_{i2}^j \in PR$	*Формальные описания процессов*: множество бинарных правил, описывающих допустимые в узловых точках системы последовательности выполняемых процессов
FO	$\{FO_1, FO_2, ..., FO_f\}$, где FO_i – i-е отношение $f_i^1(\{O_{i1}^1\}) * f_i^2(\{O_{i2}^2\})$, а $* \in \{(=) \vee (\neq) \vee (\geq) \vee (>)\}$	*Функциональные отношения*: формальные описания установленных в системе функциональных отношений между объектами

4. Определения и обозначения взаимосвязей субъектов и объектов по видам доступа

При построении модели используется пять типов доступа субъектов к объектам, образующие множество A и определенные как атрибуты доступа:

$\underline{r}$ – для чтения;

$\underline{a}$ – с присоединением;

$\underline{e}$ – с выполнением;

$\underline{w}$ – для записи;

$\underline{c}$ – с контролем.

Опишем их более подробно.

Доступ для чтения – чтение объекта субъектом (получение субъектом данных, содержащихся в объекте). Доступом для чтения к объекту нельзя воздействовать на содержимое этого объекта. Этот режим доступа дает субъекту возможность обращаться к файлу, содержащему информацию, о которой можно получить справку, но которая не может быть им изменена. Примером такой информации являются данные о классификации и доступности субъектов и объектов в системе. В процессах, связанных с созданием и использованием ЭД, эта информация должна быть доступна и неизменна. Доступ только для чтения обеспечивает соответствующую комбинацию доступности и защиты.

Доступ с присоединением – модификация данных объекта субъектом без их предварительного прочтения. Доступ с присоединением позволяет изменять объект (в частности, добавлять информацию к формируемому ЭД) с предотвращением извлечения информации из него. Таким образом, доступ с присоединением к формируемому ЭД не предоставляет субъекту содержимое ранее сформированной его части. Доступ с присоединением может обозначать операцию записи в файл, содержащий фрагмент формируемого ЭД.

Доступ с выполнением – исполнение субъектом объекта (действие, не связанное ни с чтением, ни с модификацией данных). Доступ с выполнением позволяет субъекту только вызывать выполняемый объект типа программы или подпрограммы. Обычный пользователь не может читать или писать программу, а имеет возможность только осуществить доступ с выполне-

нием. Если вызванная программа производит информацию, которая передается обратно вызвавшей программе, то это должно осуществляться под контролем системы. Если данный вид доступа используется для программы, результаты выполнения которой записываются в файл для последующего чтения вызвавшей ее программой, а произведенная информация была классифицирована выше, чем уровень классификации вызывающей программы, то система должна отвергнуть доступ для чтения вызывающей программы к файлу, в котором сгенерированная информация была сохранена.

Доступ для записи – запись-модификация данных объекта после их предварительного прочтения субъектом. Для простоты будем называть этот тип доступа доступом для записи. Доступ для записи – тип доступа, который использовался бы при редактировании или модифицировании файла, содержащего формируемый ЭД или фрагмент формируемого ЭД.

Доступ с контролем предназначен для формализации понятия контроля над объектом и доступа к нему. Используется при изменении прав доступа, которыми владеет субъект S_i по отношению к объекту O_j, другому субъекту S_k. Доступ с контролем может использоваться субъектом для блокировки и разблокировки файла по отношению к другому субъекту.

Для контроля прав доступа обычно используются матрицы доступа, элементы которых определяют условия доступа каждого субъекта $S_i \in S$ к каждому объекту $O_j \in O$ (рисунок). Каждый элемент M_{ij} матрицы доступа M определяет права доступа i-го субъекта к j-му объекту (читать, писать, выполнять, нельзя использовать и т. п.). Элементы в матрице доступа имеют следующие значения: r – чтение, w – запись, e – выполнение, 0 – нельзя использовать.

Субъекты	Объекты					
	O_1	O_2	…	O_9	…	O_n
S_1	0	$\underline{wc}$		$\underline{r}$		$\underline{wc}$
S_2	$\underline{wc}$	0		0		0
…						
S_6	0	0		$\underline{rwc}$		
…						
S_m	$\underline{e}$	$\underline{e}$		0		$\underline{e}$

Рис. Пример матрицы доступа

Элементы матрицы доступа могут содержать указатели на специальные процедуры, которые должны выполняться при обращении субъекта к объекту. Решение о доступе в этом случае основывается на результатах выполнения данных процедур, например:

– на анализе предыдущих доступов к другим объектам;

– динамике состояния системы (права доступа субъекта зависят от текущих прав доступа других субъектов);

– значении определенных переменных, например на значении таймера.

Необходимо отметить, что строка $M[S_i,*]$ содержит список разрешенных операций субъекта S_i по отношению ко всем объектам, а столбец $M[*,O_j]$ определяет, какие субъекты имеют права доступа к объекту O_j и какие именно права доступа.

Размерность матрицы доступа существенно зависит от количества субъектов и объектов в системе, поэтому для уменьшения размерности матрицы доступа могут применяться различные методы:

– установление групп субъектов, каждая из которых представляет собой группу субъектов с одинаковыми правами;

– группировка объектов по уровням категорий (например, по уровням секретности);

– хранение списка пар вида (O_j, PA_i), где O_j – определенный объект, PA_i – разрешение на использование его субъектом S_i.

5. Определения и обозначения запросов субъектов по управлению доступом к объектам

В процессе моделирования будем рассматривать четыре типа запросов, образующих множество RA и содержащих требования, предъявляемые к системе:

q: разрешить, предоставить – требование субъекта предоставить доступ к объекту в определенном режиме;

r: запретить, отменить – требование субъекта отменить атрибуты доступа к какому-нибудь объекту для другого субъекта;

c: изменить, создать – требование субъекта создать объект в системе;

d: удалить – требование субъекта удалить объект из системы.

Для запросов типа q $(q \in RA)$ имеют смысл только требования для предоставления прав на чтение, запись, присоединение или выполнение. Атрибут контроля доступа предлагается использовать таким образом, чтобы запрос субъекта на предоставление контроля над объектом не имел бы никакого смысла. Следовательно, при использовании запроса данного типа субъект может требовать только доступ для чтения, записи, выполнения и присоединения к объекту. Когда такое требование предъявлено, системой должен быть сделан ряд проверок. Одна из них, и, возможно, наиболее очевидная, – проверить, имеет ли субъект право на обращение к объекту в запрашиваемом режиме. Она выполняется путем проверки матрицы доступа. Например, субъект S_1 может запрашивать доступ с правом на запись к объекту O_2 в соответствии с матрицей доступа, представленной на рисунке, но если субъект S_1 запросит доступ на выполнение к объекту O_2, то данный запрос будет рассматриваться системой как запрос, не соответствующий установленным для данного субъекта полномочиям. После этого должны быть выполнены другие проверки прежде, чем системой будет принято окончательное решение. Они должны выполняться с целью сохранения системой специальных свойств и условий правомочности выполняемых действий, которые будут определены позже.

Для запросов типа r $(r \in RA)$ также требуется выполнение ряда условий. Представим требование субъекта S_6 для отмены доступа по чтению ($\underline{r}$, где $\underline{r} \in A$) субъекту S_2 относительно объекта O_9. Данное требование, например, может предшествовать требованию на изменение содержимого O_9 субъектом S_6. При принятии системой решения о правомочности требования субъекта S_6 на отмену доступа по чтению субъекта S_2 к объекту O_9 прежде всего осуществляется проверка того, что матрица доступа содержит запись, устанавливающую доступ с контролем ($\underline{c}$, где $\underline{c} \in A$) для (S_6, O_9). Эта запись означает, что субъект S_6 сам имеет права на доступ с контролем к объекту O_9. Далее осуществляется проверка того, что субъект S_6 также обладает правами доступа к объекту O_9, которые он требует отменить для субъекта S_2. В данном случае субъект S_6 непосредственно должен иметь атрибут доступа по чтению к объекту O_9. Таким образом, субъект не может отменять или предоставлять атрибуты доступа к объекту другим субъектам, если он сам не имеет доступ с контролем к этому объекту, и соответствующие атрибуты доступа, которые он пытается отменить или предоставить. Кроме того, будем запрещать субъекту распространять атрибут контроля доступом на другой субъект. Окончательное решение о правомочности предъявленного требования принимается системой после проведения дополнительных проверок, которые будут рассмотрены позже.

Для запросов типа c $(c \in RA)$ под действиями, запрошенными на создание объекта, предлагается понимать включение неиспользуемого объектного индекса в множество объектных индексов текущего состояния. Это позволяет избежать потребности в динамическом изменении размерности матрицы доступа M и функций классификации f. Активация объектного индекса логически эквивалентна добавлению нового объекта в множество O^+. Отметим, что в модели каждый объект, активный или неактивный, имеет назначенные ему классификацию и набор категорий. Поэтому если классификация и набор категорий у создаваемого таким образом объекта O_j не удовлетворяют требованиям имеющих к нему доступ активных субъектов, то данный запрос должен быть отвергнут системой как неправомочный. Запросы этого типа не изменяют классификаций или категорий активных объектов и не изменяют условия доступа или категории субъектов, а также не модифицируют текущее распределение объектов по отношению к субъектам. Таким образом, требование на изменение классификации активного объекта или требование на создание объекта, который является в настоящее время активным, должны отклоняться как неправомочные.

Для запросов типа d $(d \in RA)$ под действиями, запрошенными на удаление объекта, предлагается понимать исключение соответствующего ему объектного индекса из множества объектных индексов текущего состояния. Требование удалить объект O_j может исходить только от субъекта, обладающего контролем доступа над объектом. При установлении правомочности данного требования результат его выполнения делает O_j неактивным и немедленно отменяет все текущие права доступа к O_j.

6. Определение образа системы и ее корректного состояния

В процессе функционирования системы множества субъектов и объектов, определяющих ее текущее состояние, могут динамически изменяться. Данные изменения, например, происходят в результате образования новых или уничтожения существующих субъектов или объектов, изменения прав доступа субъектов к объектам. Соответственно в процессе функционирования системы должны изменяться и данные, отражающие ее текущее состояние и обозначаемые следующим образом:

S^+ – текущее множество активных субъектов;

O^+ – текущее множество активных объектов.

Как уже говорилось ранее, системой выполняются только запросы на доступ субъектов к объектам или на управление данным доступом, содержащие требования, правомочность которых подтверждена соответствующими проверками.

Таким образом, системой должны выполняться только те требования, которые в ней определены как правомочные для того, чтобы ни компрометация, ни какая-нибудь другая проблема, связанная с правомочностью создаваемых и используемых в ней ЭД, не могла возникнуть.

Два основных ответа, которые должна выдать система в процессе принятия решения о правомочности поступившего запроса, – **да** и **нет**. Ответ **да** – требование допускается, ответ **нет** – требование не допускается. Кроме того, в данной модели определяются ответы **ошибка** и **?** (вопрос). Ответ **ошибка** указывает, что механизм принятия решения по какой-то причине нарушен, и, как правило, используется при отладке системы на начальных стадиях. Ответ **ошибка** указывает, что два или больше определенных в системе правила соответствуют одному и тому же запросу. Ответ **?** указывает, что запрос не распознан. В рассматриваемой модели это просто означает, что никакое точное правило не применимо к сделанному запросу. Ответ **?** может использоваться как внутренний ответ системы, предшествующий ответу **нет**.

Начальное и все последующие состояния, в которых может находиться моделируемая система, определим таким образом, чтобы они включали в себя всю информацию, относящуюся к сохранению правомочности создаваемых и используемых в системе ЭД.

Состояние $v \in V$ – упорядоченный кортеж

$$(b^v, M^v, f^v, PO^v, PR^v, FO^v),$$

где $b^v \in P(S \times O \times A)$ – указывает, какие субъекты имеют доступ к каким объектам и в каком режиме в состоянии v;

$M^v \in M$ – указывает элементы матрицы доступа в состоянии v;

$f^v \in F$ – указывает уровень допустимости всех субъектов, уровень классификации всех объектов и категории, связанные с каждым субъектом и объектом в состоянии v;

PO^v – указывает множество допустимых для формирования объектов бинарных правил в состоянии v;

PR^v – указывает множество допустимых в конкретной узловой точке системы выполняемых действий в состоянии v;

FO^v – указывает множество установленных в системе функциональных отношений между объектами в состоянии v.

Далее определим следующее:

– $O \in PO^v$ в том и только в том случае, когда истинно утверждение

$$(\exists(< O_i >::=< O_{i1}^j >< O_{i2}^j >) \in PO^v) \Rightarrow (O_i \in O^+) \wedge (((O_{i1}^j = O) \vee ((O_{i1}^j \in O^+) \wedge (O_{i2}^j = O)) \vee$$
$$\vee ((< O_i >= O) \wedge (O_{i1}^j \in O^+) \wedge (O_{i2}^j \in O^+)));$$

– $O \in FO^v$ в том и только в том случае, когда истинно утверждение

$$\forall(FO_i = f_i^1(\{O_{i1}^1\}) * f_i^2(\{O_{i2}^2\}) \in FO^v) \Rightarrow \forall O \in (\{O_{i1}^1\} \cup \{O_{i2}^2\}) \Rightarrow O \in O^+).$$

Пусть $W \subseteq R \times D \times V \times V = \{(r, d, v_2, v_1)\}$, где (r, d, v_2, v_1) – действие системы, определяемое следующим образом: система находилась в состоянии v_1, поступил запрос r, по которому принято решение d, и система перешла в состояние v_2.

Пусть T – множество значений времени (для удобства будем считать, что T эквивалентно множеству натуральных чисел). Определим набор из трех функций (x, y, z)

$$x : T \to R,$$
$$y : T \to D,$$
$$z : T \to V$$

и обозначим множества таких функций X, Y, Z соответственно.

С учетом введенных обозначений $(x, y, z) \in \sum(R, D, W, z_0)$ далее будем называть образом системы.

Определим, что $x \in PR^v$ в том и только в том случае, когда истинно утверждение

$$(\exists(< PR_i >::=< PR_{i1}^j >< PR_{i2}^j >) \in PR^v) \Rightarrow (PR_i \in PR^v) \wedge ((PR_{i1}^j = x) \vee$$
$$\vee((PR_{i1}^j \in PR^v) \wedge (PR_{i2}^j = x))).$$

В соответствии с данными обозначениями и определениями моделируемая система представляется как

$$\sum(R, D, W, z_0) \subset X \times Y \times Z.$$

При этом $(x, y, z) \in \sum(R, D, W, z_0)$ тогда и только тогда, когда $(x_t, y_t, z_t, z_{t-1}) \in W$ для каждого $t \in T$, где z_0 – обычно определенное начальное состояние системы (ϕ, M, f) и ϕ обозначает пустое множество.

Таким образом, W определяется как объединение отдельных действий, выполняемых в процессе функционирования системы по поступающим запросам и результатам проверок, проведенных системой с целью сохранения правомочности создаваемых и используемых в ней ЭД. Проводимые проверки должны обеспечивать выполнение условия правомочности текущих состояний, в которых может находиться система, и сохранять характеристику системы, определенную как свойство правомочности.

Условие правомочности определяется следующим образом: $(S, O, \underline{x}) \in S \times O \times A$ удовлетворяет условию правомочности относительно f^v в том и только в том случае, когда

$$((O \in FO^v) \wedge (O \in PO^v) \wedge (\underline{x} \in PR^v))$$

и $$((\underline{x} = \underline{e}) \vee (\underline{x} = \underline{a}) \vee (\underline{x} = \underline{c}))$$

или $$((\underline{x} = \underline{r}) \vee (\underline{x} = \underline{w})) \wedge (f_1(S) \geq f_2(O)) \wedge (f_3(S) \supseteq f_4(O)).$$

Состояние $v \in V$ – правомочное состояние тогда и только тогда, когда каждое $(S, O, \underline{x}) \in b^v$ удовлетворяет условию правомочности. Состояние v – компромиссное состояние (компромисс) тогда и только тогда, когда оно не является правомочным состоянием.

Последовательность состояний $z \in Z$ имеет компромисс в том и только в том случае, когда z_t для некоторого $t \in T$ является компромиссным состоянием. Последовательность состояний z является последовательностью правомочных состояний тогда и только тогда, когда z_t – правомочное состояние для каждого $t \in T$.

Определим, что $(x, y, z) \in \sum(R, D, W, z_0)$ – правомочный образ тогда и только тогда, когда z – последовательность правомочных состояний.

Образ (x, y, z) имеет компромисс тогда и только тогда, когда z имеет компромисс.

$\sum(R, D, W, z_0)$ – правомочная система тогда и только тогда, когда каждый образ $\sum(R, D, W, z_0)$ правомочен.

$\sum(R, D, W, z_0)$ имеет компромисс тогда и только тогда, когда некоторый образ $\sum(R, D, W, z_0)$ имеет компромисс.

С целью сокращения дальнейших выкладок введем следующие понятия. Пусть $b^v(S : \underline{x}, \underline{y}, ..., \underline{z})$ обозначает множество

$$\{O : O \in PO^v \wedge [(S, O, \underline{x}) \in b^v \vee (S, O, \underline{y}) \in b^v \vee ... \vee (S, O, \underline{z}) \in b^v]\}.$$

Свойство правомочности определяется следующим образом.

Состояние $v = (b^v, M^v, f^v, PO^v, PR^v, FO^v) \in V$ удовлетворяет свойству правомочности тогда и только тогда, когда для каждого $S \in S^+$ утверждение

$$[[b^v(S : \underline{w}, \underline{a}) \neq \phi \wedge b^v(S : \underline{r}, \underline{w}) \neq \phi] \Rightarrow$$
$$[(((\underline{w}, \underline{a}) \in PR^v) \wedge ((\underline{r}, \underline{w}) \in PR^v)) \wedge (\forall((O_1 \in b^v(S : \underline{w}, \underline{a})) \wedge (O_1 \in PO^v) \wedge (O_2 \in b^v(S : \underline{r}, \underline{w})) \wedge$$
$$\wedge(O_2 \in PO^v)) \wedge (f_2(O_1) \geq f_2(O_2)) \wedge (f_4(O_1) \supseteq f_4(O_2))]]$$

истинно.

Состояние v нарушает свойство правомочности тогда и только тогда, когда v не удовлетворяет свойству правомочности.

Последовательность состояний $z \in Z$ удовлетворяет свойству правомочности тогда и только тогда, когда z_t удовлетворяет свойству правомочности для каждого $t \subset T$.

$(x, y, z) \in \sum(R, D, W, z_0)$ удовлетворяет свойству правомочности тогда и только тогда, когда z удовлетворяет свойству правомочности.

$\sum(R, D, W, z_0)$ удовлетворяет свойству правомочности тогда и только тогда, когда каждый образ $\sum(R, D, W, z_0)$ удовлетворяет свойству правомочности.

В процессе функционирования системы переходы из одного состояния системы в другое должны осуществляться в соответствии с установленными в системе правилами перехода.

Корректное состояние системы определяется как состояние системы, одновременно удовлетворяющее условию и свойству правомочности.

7. Определение корректных правил перехода

Правила перехода – это определенный в системе набор правил, каждое из которых устанавливает определенную в системе последовательность функциональных действий, обозначаемую как ρ: $R \times V \to D \times V$. Смысловая интерпретация правила ρ определяется следующим образом: получив данный запрос и состояние, система выполняет определенную соответствующим правилом последовательность функциональных действий, в результате которых принимается решение об изменении состояния системы и происходит изменение состояния. Правило аналогично конкатенации функций ввода, обработки и вывода (в каждом последующем состоянии) в последовательно действующей машине.

Правило ρ сохраняет правомочность состояний тогда и только тогда, когда утверждение [[$\rho(R_k, v) = (D_m, v^*)$ и v – правомочное состояние] влечет, что [v^* – правомочное состояние]] справедливо для всех элементов $(R_k, v) \in (R \times V)$ при условии, что $(\underline{x} \in RA \in R_k) \Rightarrow (\underline{x} \in PR^v) \wedge$ $\wedge((O \in V) \Rightarrow (O \in FO^v) \wedge (O \in PO^v))$. Правило ρ сохраняет свойство правомочности тогда и только тогда, когда утверждение [[$\rho(R_k, v) = (D_m, v^*)$ и v удовлетворяет свойству правомочности] влечет, что [v^* удовлетворяет свойству правомочности]] справедливо для всех элементов $(R_k, v) \in (R \times V)$ при условии, что $(\underline{x} \in RA \in R_k) \Rightarrow (\underline{x} \in PR^v) \wedge ((O \in V) \Rightarrow (O \in FO^v) \wedge$ $\wedge(O \in PO^v))$.

Правило перехода является корректным, если при его применении система переходит из текущего корректного состояния в последующее корректное состояние.

Пусть $\omega = \{\rho_1, \rho_2, ..., \rho_s\}$ – множество правил относительно R, D и V. Отношение $W(\omega)$ определяется следующим образом:

(i) $(R_k, \mathbf{?}, v, v) \in W(\omega)$ тогда и только тогда, когда $\rho_i(R_k, v) = (\mathbf{?}, v)$ для каждого i, $1 \le i \le s$;

(ii) $(R_k,$ **ошибка,** $v, v) \in W(\omega)$ тогда и только тогда, когда существуют i_1, i_2, $1 \le i_1 \le i_2 \le s$, такие, что $\rho_{i_1}(R_k, v) \ne (\mathbf{?}, v^*)$ и $\rho_{i_2}(R_k, v) \ne (\mathbf{?}, v^{**})$ для некоторых $v^*, v^{**} \in V$;

(iii) $(R_k, D_m, v^*, v) \in W(\omega)$ тогда и только тогда, когда существует единственное i, $1 \le i \le s$, такое, что $(\mathbf{?}, v^{**}) \ne \rho_i(R_k, v) = (D_m, v^*)$ для некоторого v^* и любого другого $v^{**} \in V$.

Можно интерпретировать правило как формальную реализацию интуитивного понятия того, как система обрабатывает запросы, выдавая ответы, основанные на особенностях текущей ситуации и обрабатываемого запроса. Если правило ρ_i не обрабатывает запрос R_k, то

$\rho_i(R_k, v) = (\mathbf{?}, v^*)$. Это означает, что ρ_i не применимо к (R_k, v). Если для некоторого (R_k, v) не применимо ни одно из правил, то $W(\omega)$ не применимо и ответ системы – (**?**,*v*) по (i) определению $W(\omega)$. При определении $W(\omega)$ будем требовать, чтобы каждый тип запроса мог быть обработан не более чем одним правилом. Если применимо больше чем одно правило, то ответ системы – (**ошибка**, *v*) по (ii) определению $W(\omega)$. Если только одно правило применимо к (R_k, v) с получением в результате (D_m, v^*), то ответ системы – (D_m, v^*) по (iii) определению $W(\omega)$.

По аналогии с [4] можно определить набор правил перехода, обеспечивающих обработку поступающих в систему запросов на выполнение определенных действий, и дать формальное описание самих правил с доказательством того, что функционирующая в соответствии с данным набором правил система с правомочным начальным состоянием, удовлетворяющим свойству правомочности, является правомочной и удовлетворяет свойству правомочности. Это подтверждает правомочность формируемых и используемых в ней ЭД, однако рассмотрение данных вопросов выходит за рамки настоящей статьи.

Заключение

Построение математических моделей подтверждения правомочности ЭД в процессе проектирования систем позволит их разработчикам использовать математические методы анализа свойств создаваемой системы до ее программно-аппаратной реализации. В свою очередь, применение математических методов дает возможность получения гарантий и по обеспечению корректности принимаемых технических решений. При отсутствии такой возможности вопросы корректности остаются, как правило, открытыми. Следует отметить, что в системах электронного документооборота данная проблема является весьма актуальной. Например, противоречивость решений, устанавливающих требования к структурам ЭД, множеству допустимых в узлах системы последовательностей реализуемых процессов, функциональных отношений между объектами, существенно увеличивает риск эксплуатации данных систем. В то же время использование при определении перечисленных требований формального метаязыка позволяет выявить неоднозначность описания объектов проектируемой системы еще на этапе анализа соответствующих им грамматик. Кроме того, получение абсолютных, а не вероятностных оценок свойств системы, определяющих правомочность ЭД, позволит существенно сократить затраты на их создание, гарантируя наличие и выполнение определенных в системе условий и свойств правомочности в процессе формирования и использования ЭД.

Список литературы

1. Цынкевич, Е.А. Задачи определения критериев правомочности электронных документов / Е.А. Цынкевич // Информатика. – 2005. – № 4 (8). – С. 87–93.

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

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

4. Bell, D.E. Secure Computer Systems: A Mathematical Model / D.E. Bell, L.J. La Padula // MTR-2547 Vol. II. The MITRE Corporation. – Bedford, Massachusetts, 1996.

5. Конявский, В.А. Основы понимания феномена электронного документооборота / В.А. Конявский, В.А. Гадасин. – Минск: Биллитфонд, 2004.

6. Цынкевич, Е.А. Критерии правомочности электронных документов / Е.А. Цынкевич // Материалы IX Междунар. конф. «Комплексная защита информации». – Минск, 2005, – С. 106–107.

7. СТБ 34.101.1-03. Критерии оценки безопасности информационных технологий.

8. Repot on the Algorithmic Language ALGOL 60. Communication of the Association for Computing Machinery / P. Naur [et al.]. – USA, 1960. – 299 p.

9. Маслов, Ю.Г. Проект стандарта ЭЦП организации для обеспечения юридической значимости электронного документа / Ю.Г. Маслов, А.В. Фураков // ВКСС. Connect. – М., 2006. – № 4. – С. 140–141.

10. Маккиман, У. Генератор компиляторов / У. Маккиман, Дж. Хорнинг, Д. Уортман; пер. с англ. – М.: Статистика, 1980. – 527 с.

11. СТБ 1176.1-99. Информационная технология. Защита информации. Функция хэширования.

Поступила 11.05.07

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6

Расчетный центр Национального банка
Республики Беларусь,
Минск, Кальварийская, 7
e-mail: y.tsynkevich@gmail.com

E.A. Tsynkevich

MATHEMATICAL MODEL OF ELECTRONIC DOCUMENTS COMPETENCE

A problem of securing the electronic document competence in interaction systems during document creation and execution is considered. The basic elements, states and rules of transition of the mathematical model of electronic document competence are defined. An approach of guaranteeing an electronic document interaction system state to be accepted as competent is proposed.