Серия «Библиотека журнала «УЗИ»

В. А. Конявский, В. А. Гадасин

ОСНОВЫ ПОНИМАНИЯ ФЕНОМЕНА ЭЛЕКТРОННОГО ОБМЕНА ИНФОРМАЦИЕЙ

Минск
2004

УДК

Серия основана в 2000 году

В. А. Конявский, В. А. Гадасин
Основы понимания феномена электронного обмена информацией. — Минск, 2004. — 327 с.

Рассматривается феномен электронного обмена информацией и на основе этого разрабатывается теоретическое обоснование понятий «документ», «электронный документ», строятся и изучаются модели этих явлений, предлагается программно-техническая реализация аппаратной защиты технологии информационного взаимодействия.

Для научных работников, специалистов в области электронного документооборота и его зашиты, студентов и аспирантов соответствующих специальностей.

В. А. Конявский, В. А. Гадасин
Основы понимания феномена электронного обмена информацией. — Минск, 2004. — 327 с. (Серия «Библиотека журнала «УЗИ»)

Научное издание

Редактор А. П. Леонов, С.В. Конявская

Компьютерная верстка Ю. В. Павловский

Подписано в печать __ Формат __

Гарнитура Таймс. Печать офсетная

П.л. __ Тираж __ Заказ __

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Беспрецедентное развитие вычислительной техники обусловило структурный сдвиг в сфере информационного взаимодействия. Отчуждение электронного документа от человека неуклонно возрастает — информационное взаимодействие людей замещается взаимодействием ЭВМ. Электронная «информация» лишается содержания, сведения, знания, присущего ей в человеческой среде. Компьютеру безразличен смысл документа, для него «информация» — всего лишь маркированное особым образом подмножество двоичных символов. Аналогия между традиционной и электронной технологией отображения документа, когда компьютер при создании документа использовался как «большая пишущая машинка», уже в прошлом.

Для окружающего нас мира базовыми являются две материальные категории существования — *материя* (предмет, объект) и *энергия* (процесс, сигнал). Предмет как носитель документа традиционен и не вызывает недоумения. При этом нет никаких оснований, что бы отказать в возможности такого применения процессу. В работе выделяются две формы отображения информации: аналоговая в виде объекта, предмета; электронная или цифровая в виде процесса. И в том, и в другом случае параметры *пространственного* объекта и наблюдаемые в течение конечного промежутка *времени* характеристики энергии (сигнала) должны соответствовать информационным элементам.

Для того, чтобы документ исполнял роль сообщения о факте (служил информационным фактом), необходимо обеспечить его предъявление и демонстрацию по произвольному требованию сектора действенности. Для традиционного документа характерна неизменность на всем жизненном

цикле, но для электронного это не так — допускается непосредственно для демонстрации изготовление «точно такого же» электронного документа (ЭлД).

Чтобы «успеть» изготовить документ в крайне сжатое время подготовки к демонстрации, процесс создания ЭлД должен быть автоматическим, представлять собой технологию из строго детерминированной последовательности действий во временном порядке. Можно говорить о двух формах существования технологии. В форме процесса — алгоритм операции, в форме предмета — аппаратное средство. Таким образом, технология преобразования информации и собственно информация концептуально едины.

Ресурсами для защиты информации являются избыточность как собственно информации, так и свойств объектов или процессов, достаточно «прочно» связанных с этой конкретной информацией — атрибутов документа. При аналоговой форме отображения множество точек, формирующих атрибуты, несопоставимо «больше», чем точек, отображающих информацию, тогда как при электронной форме мощность атрибутов меньше мощности информационных сигналов. Чем выше ресурс — тем больше возможностей, поэтому для защиты конкретной информации, с общих позиций, использование аналоговых атрибутов заведомо *значительно эффективнее*, чем электронных.

Математическая сущность защиты любого объекта заключается в сохранении однозначного соответствия его свойств, наблюдаемых в двух разных точках «пространство-время». Сопоставление с эталоном, пусть неявное, имеет место в любом случае. Механизмы и методы защиты собственно электронного «документа-информации» должны исходить из случайности эталона и известности реализации, тогда как защиты электронной «технологии-информации» — из случайности реализации и *известности* эталона. Эталонная технология фиксируется явными или

неявными соглашениями участников на достаточно длительное время, поэтому ее, по крайней мере, отдельные компоненты, можно реализовать в *аппаратном* виде. Приведенные качественные соображения обосновывают целесообразность смещения акцентов в область аппаратной защиты технологий электронного обмена информацией.

ВВЕДЕНИЕ

Документооборот — один из основных видов информационного взаимодействия. Действующим агентом здесь является собственно документ как совокупность сведений, а феноменом информационного взаимодействия выступает осведомление как процесс, реализуемый в системах различных типов. Исходя из природы объектов, участвующих в информационном взаимодействии, различаются три типа систем — искусственные (технические), смешанные и естественные (живые) [1]. Выделяя из всех возможных видов информационного взаимодействия в системах перечисленных типов конкретное взаимодействие — документооборот, можно зафиксировать природу участников (объектов) данного взаимодействия.

Наиболее известным является документооборот в естественных системах — в качестве такового можно рассматривать документооборот в любых уровнях социальных сообществ. На предприятиях, корпорациях, в государствах и др. документооборот осуществляется в качестве процесса осведомления участников информационного взаимодействия. Для естественных систем таковыми являются люди. При этом можно выделить условия успешного информационного взаимодействия – нужно не только передать сообщение, но и необходимо обеспечить условия, при которых адресат сумеет адекватно воспринять его.

Достигается это наличием доступной участникам согласованной априорной информации, достаточной для выделения полученного сообщения из множества сигналов и его усвоения — принцип тезауруса. Техническими средствами, участвующими в документообороте такого типа, можно пренебречь: авторучка, пишущая машинка, лазерный принтер являются лишь пассивными средствами изготовления документа. Правила изготовления исполняются людьми, документооборот в естественных

системах осуществляется по схеме «человек – человек», или, как мы будем говорить далее, «Субъект – Субъект (С – С)».

Другая ситуация в искусственных (технических) системах: от простейших регуляторов до глобальных компьютерных сетей. Прежде всего, здесь стоит остановиться на известных видах информационного взаимодействия в целом. На сигнальном уровне информационное взаимодействие описывается энтропийным подходом [2], на лингвистическом — алгоритмическим [3] и алгебраическим (комбинаторным) [4] подходами. Нельзя не отметить и подход при описании ситуаций «управляющий объект – управляемый объект» [5], который требует рассмотрения соответствующих целей управления.

Важнейшим моментом последнего является то, что энергетические характеристики полученного приемником сигнала играют второстепенную роль. Гораздо более существенной характеристикой является форма сигнала, отражающая его информационное содержание. Изменение формы сигнала меняет информационное содержание, и цель информационного взаимодействия может быть не достигнута. В связи с этим можно утверждать, что важнейшим условием успешного информационного взаимодействия в технических системах является условие сохранения формы сигнала.

Для цифровых систем форма сигнала отражается последовательностью бит – нулей и единиц в принятой системе кодирования. Следовательно, задача сохранения формы сигнала в цифровой среде эквивалентна (с точностью до системы кодирования) задаче сохранения порядка. Таким образом, при документообороте в технических системах и источником, и приемником являются технические (аппаратные и программные) средства, а агентом взаимодействия — электронный документ (ЭлД), характеризуемый формой и порядком информационных элементов. Будем далее говорить, что документооборот

в технических системах осуществляется по схеме «техническое средство – техническое средство», или «Объект – Объект (О – О)».

Наиболее актуальным в настоящее время является изучение информационного взаимодействия (и документооборота как одной из его форм) в системах смешанного типа. Сюда относятся информационные взаимодействия типа «живой организм – искусственный орган», «человек – машина», «живой исследователь – неживой объект исследования» и др. Именно такие системы получают сегодня наиболее широкое распространение. В системах данного класса появляются еще два типа взаимодействия, а именно: «Субъект – Объект (С – О)» и «Объект – Субъект (О – С)».

Эти типы взаимодействия представляют собой в определенном смысле «интерфейсы» между аналоговым миром людей и цифровым «миром» технических систем, обеспечивая «вход» человека в техническую систему и «выход» из нее. Хорошим примером такой системы является банковская система выдачи наличных денег по пластиковой карте – субъект инициирует процесс выработки в технической системе потока электронных документов, позволяющих установить его права на получение денег (взаимодействие «С – О»). Этот процесс осуществляется полностью без участия человека, в технической системе (взаимодействие «О – О). В случае положительного решения, вырабатываемого технической системой, банкомат (технический объект) выдает деньги человеку (взаимодействие «О – С»).

При исследовании электронного документооборота помимо анализа традиционного взаимодействия «С – С» необходимо изучить взаимодействие «О – О», а затем расширить полученную схему интерфейсными блоками взаимодействия: «С – О» и «О – С».

Анализ известных моделей защиты информации показал, что в подавляющем большинстве подходов рассматривается лишь «доступ

субъекта к объекту». Более того, в качестве аксиомы предлагается принять предположение о том, что «все вопросы безопасности в автоматизированной системе описываются доступами субъектов к объектам». В [6] подчеркивается, что «нас не интересует, какую задачу решает система, мы лишь моделируем ее функционирование последовательностью доступов». При такой постановке полностью игнорируются состав и структура вычислительной системы, и даже различия собственно объектов защиты. Представляется, что различия между такими объектами защиты, как компьютер, операционная система, информационная технология, сеть передачи данных, объекты файловой системы, электронные документы, — достаточно значимы для того, чтобы их учитывать.

Понятия упорядоченности, (вычислимого) изоморфизма являются фундаментальными для защиты электронного информационного обмена. Причем это относится не только к собственно информации — фиксированной последовательности двоичных сигналов, но и к технологии реализации документооборота — протокол взаимодействия есть ни что иное, как строго упорядоченная последовательность операций. Преобразование информации, например, при изменении формата, меняет формальный порядок в последовательности, но сохраняет упорядоченность. Изменение технологии, например, при смене операционной системы, меняет реализацию команд, но, как и ранее, сохраняет их упорядоченность.

С прикладной точки зрения необходимо обеспечить условия, при которых в процессе создания и обработки электронных документов (вычислимый) изоморфизм собственно преобразований и изоморфизм множества сигналов, маркированного как «информация», будут сохраняться. Существенно, что если каждое преобразование из множества применяемых в процессе обработки электронного документа сохраняет его

(документа) изоморфизм, то в силу свойства транзитивности сохраняет изоморфизм и вся совокупность (технология) преобразований. Таким образом, электронный документ нельзя рассматривать в отрыве от электронной среды. Защита ЭлД необходимо должна включать и защиту технологии — факторов, инвариантных «содержанию» ЭлД, не зависящих от него, т. е. непосредственно фрагмента электронной сети.

Говоря о защите электронных документов, мы должны рассмотреть не только собственно ЭлД, но и этапы обеспечения неизменности программно-технического комплекса объекта информатизации, генерации и поддержки изолированной программной среды — т. е. методы контроля и поддержания неизменности электронной среды существования ЭлД. Неизменность ЭлД должна обеспечиваться стабильностью свойств информационной технологии, выбранной для его обработки взаимодействующими субъектами. Это означает, что использованная технология должна соответствовать эталонной технологии, свойства которой были предварительно исследованы и признаны удовлетворяющими требованиям безопасности. Понимая информационную технологию (ИТ) как упорядоченное множество операций, можно назвать ИТ, обладающую свойством сохранять упорядоченность множества операций, защищенной.

Материальную реализацию изделия-документа называют носителем информации или носителем документа. Само по себе изделие необходимо должно быть феноменом материального мира. Оно характеризуется объективно существующей системой физических измерений параметров изделия. Таким образом, система чисел — параметров данного изделия, считанная в определенном порядке, вполне «пригодна» для отображения информации, носителем которой это изделие является. Здесь мы опять сталкиваемся с понятием порядка при определении информации. Отправной точкой для различения порядка параметров функционально

служит изделие. Заметим, что собственно информация нематериальна, что вполне отвечает, например, ее отображению в виде совокупности также нематериальных чисел — результатов физического измерения параметров изделия. (Отображение информации буквенным текстом представляет собой частный случай цифрового отображения — количество различных «цифр» равно суммарному количеству разных букв, обычных цифр, пробелов, знаков препинания и т. п.).

Документ как изделие может рассматриваться как посредник (агент) информационного взаимодействия. В правовой сфере есть понятие [7] *юридический факт* — предусмотренные в *законе* обстоятельства, при которых сохраняются или изменяются (возникают, прекращаются) конкретные правоотношения. Признание документа сообщением о факте в социальной среде обеспечивается силой — обществом в лице государства или правилами и обычаями определенной социальной группы, называемой сектором действенности документа. Эта высшая относительно любого из участников инстанция, используя свои институты поощрения и наказания, предопределяет однозначную интерпретацию содержания, диктует реакцию участников информационного обмена на документ, предоставляет им права и налагает обязанности.

Для того чтобы документ исполнял роль информационного факта, необходимо обеспечить его предъявление и демонстрацию по требованию сектора в *произвольные* моменты времени и в *неопределенных* заранее точках пространства. Демонстрация документа предполагает, что заданные характеристики предъявленного изделия не зависят от точки «пространство — время» — совпадают с параметрами эталона, существовавшего в исходной точке.

Основным преимуществом традиционных технологий изготовления и применения предмета в качестве носителя документа является неизменность (фиксированность) его параметров в течение *длительного*

времени при достаточно широком диапазоне условий окружающей среды. Энергетические и пространственные ресурсы, требуемые для такой реализации документа, как правило, незначительны. Это свойство позволяет достаточно просто обеспечить требованием перемещения во времени — хранения изделия-документа в течение жизненного цикла. Но очевидны и недостатки традиционной технологии, краеугольным из которых является низкая скорость перемещения документа в пространстве. Недостаток низкой скорости органичен, а поскольку документ в форме предмета имеет бесконечное множество точек (но с конечным числом измеримых характеристик — т. е. информации!) радикальных способов его преодоления в рамках традиционных технологий не существует.

Выход, если он существует, возможен только на принципиально ином пути — передаче объекта «по частям», дезинтеграции на отображение информации на месте отправления и последующей их интеграции на месте приема. А это означает отказ от передачи характеристик материального носителя документа как предмета, их «слишком много». В то же время любое сообщение всегда может быть отображено конечным числом параметров (знаков). Так как предметом является конечное число точек измеримых характеристик документа, то предложенный способ, по меньшей мере, концептуально ведет к снижению размерности. Учитывая конечность характеристик, разумно было бы применить принцип разделения множества характеристик по времени. Таким образом, сообщение передается в виде *процесса*, занимающего конечный промежуток времени. Кардинальное отличие новых информационных технологий от технологий традиционных заключается в том, что они базируются на *изготовлении* сообщения (документа).

Из физических законов следует, что таким образом решается проблема транспортировки информации в пространстве, но сохраняется во времени — энергия быстро рассеивается. Информация индицируется как

факт только при демонстрациях, суммарное время которых несопоставимо меньше жизненного цикла. Отсюда следует, что требование постоянства документа в течение жизненного цикла явно завышено. Какое нам дело, изменяется ли документ при хранении или передаче, и даже существует ли он в промежутке между последовательными демонстрациями! Для традиционного документа подобные предположения кажутся абсурдными, но для электронного документа это уже принципиально.

Для хранения во времени необходим, согласно вышесказанному, перевод информации в форму предмета. А почему не допустить возможность не изменения формы хранения документа, а изготовления «точно такого же» документа непосредственно для данной демонстрации? Первичным является энергетическое воздействие, и в общем случае ЭлД в аналоговой форме должен *изготавливаться* на рабочем месте пользователя. Очевидно, что процесс изготовления ЭлД в аналоговой форме должен быть автоматическим, иначе все преимущества высокой скорости транспортировки документа теряются. Ведь пользователь воспринимает только традиционное отображение информации, доступное органам чувств человека, пользователю нужен документ, ему нет дела, в какой форме он реализован.

В работе выделяются две формы отображения информации: аналоговая, в виде *объекта*, предмета; электронная или цифровая в виде *процесса*. И в том, и в другом случае наблюдаемые характеристики объекта или регистрируемые в течение конечного промежутка времени характеристики процесса должны взаимно однозначно соответствовать информационным элементам. Традиционный документ — всегда объект: например, лист бумаги, поверхность которой раскрашена совокупностью узоров, отождествляемых мышлением человека с очертанием букв. Электронный документ в активном состоянии — всегда процесс. Например, процесс появления на контактах кинескопа циклической

последовательности электрических сигналов разного потенциала инициирует появление на экране точек различной яркости. Высокий потенциал соответствует белой точке на экране, низкий потенциал — черной.

В защите информации можно выделить два качественно разных направления: *защита объектов*, т. е. собственно информации; *защита процессов* преобразования информации — технологий, инвариантных к защищаемой информации.

Отмеченное концептуальное единство (требование изоморфизма) технологии преобразования информации и собственно информации позволяет при решении проблем защиты информации рассматривать технологию с тех же позиций, что и данные. Но тогда можно также говорить о двух формах существования технологии: в форме процесса — программируемая последовательность управляющих сигналов (команд) в течение времени преобразования информации; в форме объекта — аппаратное средство, наблюдаемые характеристики которого (выходной сигнал как функция входного) однозначно определяются только алгоритмом операции, реализованном в *материальной* физической структуре средства. Как и в случае с информацией, потенциал защиты *аппаратной* реализации алгоритма много выше, чем *программной*.

Сущность защиты любого объекта заключается в сохранении однозначного соответствия его свойств, наблюдаемых в двух разных точках «пространство-время». Защита объекта абсолютна, если гарантируется, что характеристики объекта, измеряемые в любой точке (x, y, z, t) точно такие же, как в эталонной точке (x_0, y_0, z_0, t_0). Но идеал недостижим, абсолютная гарантия невозможна, всегда возможно нарушение защищенности объекта — различие характеристик в точках наблюдения. Поэтому защищенность необходимо должна индицироваться,

и, значит, сопоставление с эталоном необходимо осуществляется, сопоставление с эталоном, пусть неявное, имеет место в любом случае.

Специфика собственно информации (сообщения, документа) и технологии преобразования как информации обусловливает и специфику индикации их защищенности. В первом случае получатель документа исчерпывающе осведомлен о характеристиках объекта в точке наблюдения (x, y, z, t), но имеет мало сведений о характеристиках информации в эталонной точке (x_0, y_0, z_0, t_0) — подлинном содержании документа отправителя. Это возможно только за счет избыточности информационного обмена: предварительная договоренность, контекст информации, тематика и стиль изложения и т. п. *Известна фактическая информация, почти неизвестна эталонная*.

Во втором случае, напротив, получатель полностью осведомлен об эталонной технологии, которая признана участниками достаточно защищенной и предписана для применения. Но субъекты конкретного взаимодействия имеют крайне мало сведений, какая же технология преобразования и передачи информации была фактически использована, отличается ли текущая технология от эталонной, например, включением дополнительных операций копирования и переадресации. Разве только за счет избыточности технологии отображения информации: контекст взаимодействия, способ упаковки документа, оформление, почерк, рельефность печати, водяные знаки, способ доставки и т. п. *Известна эталонная технология, почти неизвестна фактически использованная.*

Механизмы и методы защиты собственно электронного «документа-информации» должны исходить из случайности эталона и известности реализации, тогда как защиты электронной «технологии-информации» — из случайности реализации и *известности эталона*. Только в последнем случае возникает предпосылка использования аналоговых методов и механизмов защиты: эталонная информационная технология фиксируется

явными или неявными соглашениями участников на достаточно длительное время, поэтому ее, по крайней мере, отдельные компоненты, можно реализовать в аппаратном виде. Поскольку аппаратная реализация неминуемо сопровождается потерей универсальности, гибкости, адаптируемости, управляемости, то на практике подобное целесообразно только для сравнительно простых процедур. Если эти процедуры играют ключевую роль в обеспечении безопасности технологии электронного обмена информацией, то их аппаратная реализация позволяет качественно повысить уровень защищенности — потенциал аналоговых методов и механизмов защиты информации несопоставимо выше, чем программных.

Глава 1. **АНАЛИЗ СОСТОЯНИЯ ТЕОРИИ ЗАЩИТЫ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ**

1.1. Существующая понятийная база информационного взаимодействия в электронной среде

Цель раздела — выявление современного общественного представления об электронном документе, характеристика сложившейся в обществе вербальной модели электронного документа (ЭлД). Материалы раздела отражают результаты, опубликованные в монографии [8] и работах [9–12].

Наиболее трудоемкие, сложные и дискуссионные этапы выявления общественной модели документа можно исключить, если базироваться на анализе существующих и разрабатываемых *государственных* нормативно-законодательных актов в сфере электронного документооборота. Трудно ожидать, что в этих документах могут быть радикальные положения, противоречащие сложившемуся и устоявшемуся «мнению масс», в противном случае нельзя рассчитывать на успешное прохождение законопроекта в коридорах власти. Законы и законопроекты разрабатываются высококвалифицированными специалистами, проходят многочисленную экспертизу и обсуждение на высоком уровне, так что и требования к представительности экспертов заведомо выполняются. Разумеется, субъективный фактор разработчиков и законодателей нельзя исключить, но на уровне государства его влияние, особенно в системной части законов, достаточно слабо.

Решается задача выявления сложившегося представления об электронном документе, но не конкретной оценки достоинств и недостатков самих законов, их соответствия сегодняшним требованиям. Поэтому в круг анализируемых материалов включены законопроекты, хотя

принятый закон может кардинально отличаться от представленного законопроекта.

1.1.1. Понятие «информация»

Общий анализ сущности информации и информационного взаимодействия проведен в работе [1]. Возможны различные подходы к определению информации, как с естественнонаучной точки зрения, так и с точки зрения соотнесения информации с другими научными и философскими категориями. Существует множество определений, которые условно можно разделить на 4 группы: житейское (содержательное) понимание информации; понятия, использующие формализованные модели реальных объектов и процессов; подход с позиций теории отражения и познания; учет связи информации со свойствами материи. В качестве иллюстрации, сколь многообразно варьируются подходы к определению информации в зависимости от целей анализа, приведем наиболее распространенные. Итак, информацией называют [14]:

- любые сведения о каких-либо ранее неизвестных событиях;
- содержательное описание объекта или явления;
- результат выбора;
- содержание сигнала, сообщения;
- меру разнообразия;
- отраженное разнообразие;
- сущность, сохраняющуюся при вычислимом изоморфизме;
- уменьшаемую неопределенность;
- меру сложности структур, меру организации;
- результат отражения реальности в сознании человека, представленный на его внутреннем языке;
- семантику или прагматику синтаксиса языка представления данных;

- продукт научного познания, средство изучения реальной действительности;
- основное содержание отображения;
- бесконечный законопроцесс триединства энергии, движения и массы с различными плотностями кодовых структур бесконечно-беспредельной Вселенной;
- непременную субстанцию живой материи, психики, сознания;
- вечную категорию, содержащуюся во всех без исключения элементах и системах материального мира, проникающую во все «поры» жизни людей и общества;
- свойства материи, ее атрибут; некую реалию, существующую наряду с материальными вещами или в самих вещах;
- язык мира как живого целого.

Мы не будем анализировать здесь правомерность того или иного определения, это иллюстрация отсутствия универсального подхода. Каждое из определений верно в некоторой области применения, и каждое становится неконструктивным, если оно применяется не по назначению. Говоря об электронном взаимодействии, об электронном документе, мы обязаны исходить из требования эффективности терминологии применительно к описанию электронной среды, формируемой неодушевленными объектами: программными и техническими средствами вычислительной техники и информатики. Терминология отечественных и зарубежных федеральных и государственных законов и законопроектов [15–31] в информационной сфере проанализируем как раз с позиций ее применимости при электронном взаимодействии. Приведем определения из законов и проектов законов, а затем прокомментируем их.

Федеральный закон «Об информации, информатизации, и защите информации» от 20.02.95 г. [23], ГОСТ Р 51141–98. «Делопроизводство и архивное дело. Термины и определения» [30]: — «*Информация* —

сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления».

Проект Федерального закона «Об информации, информатизации, и защите информации» от 2000 г. [18]: — «*ИНФОРМАЦИЯ — сведения о лицах, предметах, фактах, событиях, явлениях и процессах, выраженные в какой-либо объективной форме, обеспечивающей возможность их хранения и распространения*».

Проект межгосударственного стандарта ИСО/МЭК (1999 г.) [27]: — «*ИНФОРМАЦИЯ (в обработке информации) — знание (сведения) о таких объектах, как факты, события, явления, предметы, процессы, представления, включающие понятия, которые в определенном контексте имеют конкретный смысл*».

Комментарий. Лишь для общества некоторая совокупность символов, знаков, сигналов может интерпретироваться как «сведение о чем-либо», причем сам субъект необходимо должен обладать некоторой исходной системой знаний, например, умеет читать. Для неодушевленного объекта информация не «сведение» и, тем более, не «знание». Если считать, что книга, содержащая информацию, содержит «знание», то проблема приобретения знаний человеком решалась бы покупкой книг, но не их прочтением и изучением. В неживой природе объекты взаимодействуют с информационным сигналом, но не со «знанием» и «сведениями».

Знания и сведения — разные понятия. Знание — это кумулятивное свойство, оно накапливается на основе обучения и практического опыта. Разные люди имеют разные знания, тем самым из определения [27] вытекает, что информация меняется в зависимости от субъекта. В то же время, сведения относительно объективны, но неявно предполагают некоторый эталонный исходный уровень воспринимающего субъекта. Если сведения не воспринимаются, не преобразуются в знания, то это вина

конкретного субъекта, а не информации. Текст на китайском языке имеет смысл для знающего язык, но не для иностранца. На Руси любого иностранца называли «немец». Сейчас это слово называет жителя Германии, но восходит оно не к названию страны, а к слову «немой» — тот, с которым бесполезно разговаривать — невозможно получить сведения и сформировать на их основе знания. «Определенный контекст» — слишком широкое и неуловимое понятие. «Конкретный смысл» неотъемлем от субъекта, воспринимающего информацию. Более того, для разных людей эта «конкретность» может иметь совершенно разный «смысл».

Поскольку цитированные определения характеризуют информацию с позиций восприятия ее человеком, то их конструктивное использование в сфере электронного взаимодействия весьма проблематично и ведет к парадоксальным выводам. Например, поскольку компьютер не может воспринимать *сведение*, тем более — *знание*, то ЭВМ не может обрабатывать информацию. Парадокс свидетельствует, что отражаются незначимые с позиций электронного взаимодействия свойства информации. Надо исходить из инвариантных свойств информационного сигнала, а не из инвариантности семантических характеристик информации.

Машина не умеет мыслить, она умеет только преобразовывать выделенное тем или иным способом множество сигналов на основе *однозначно* заданной последовательности фиксированных операций. Для аналогового документа защита информации есть защита сведения, для электронного само сведение не имеет значения, пусть это даже бессмысленный с позиций человека набор сигналов. Для машины важна очередность информационных сигналов, и защита информации — это сохранение порядка. И это совершенно иная задача, решаемая другими методами.

Трактовка понятия «информация» в принятых законах и разрабатываемых законопроектах не соответствует перспективе массового применения электронных документов в безлюдных технологиях.

1.1.2. Понятия «документ», «электронный документ»

Здесь и далее под *аналоговым документом* (АнД) понимается традиционный документ, рассчитанный на непосредственное восприятие человеком, содержащий информацию, закрепленную на твердом носителе (бумага, фотопленка и т. д.). Выбор обусловлен присущей живому миру (значит, и человеку) способностью воспринимать информацию в аналоговой форме (изображение, звук).

Фактографическая база определений нормативных материалов федерального и государственного уровня [15–36] рассматривается как применительно к аналоговому документу, так и к электронному. Важность адекватного описания объекта правового регулирования не нуждается в доказательствах. Определения и предписания законопроектов и государственных законов России и ряда стран ближнего зарубежья в сфере электронного взаимодействия должны регулировать практическое использование ЭлД в ближайшей перспективе, их соблюдение обязательно для всех субъектов права, а их нарушение должно караться. Рассмотрим и прокомментируем определения.

Федеральный закон «Об обязательном экземпляре документов» [24]:

— «*Документ — материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования*».

Федеральный закон «Об информации, информатизации и защите информации» [23], ГОСТ «Делопроизводство и архивное дело» [30]: — «*Документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать*».

ГОСТ «Делопроизводство и архивное дело» [30]: — «*Реквизит документа — обязательный элемент оформления официального документа*»;

«*Подлинный документ — документ, сведения об авторе, времени и месте создания которого, содержащиеся в самом документе или выявленные иным путем, подтверждают достоверность его происхождения*».

«*Документ на машинном носителе — документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации ЭВМ*»;

«*Текст официального документа — информация, зафиксированная любым типом письма или любой системой звукозаписи, заключающая в себе всю или основную часть речевой информации документа*»;

«*Юридическая сила документа — свойство официального документа, сообщаемое ему действующим законодательством, компетенцией издавшего его органа и установленным порядком оформления*».

Редакция Федерального закона «Об информации, информатизации и защите информации» [18] (вариант от 2000 года) предназначена для учета технологических изменений, происшедших с момента принятия закона. В проекте утверждается: «*Электронный документ — сведения, представленные в форме набора состояний элементов электронной вычислительной техники* (ЭВТ), *иных электронных средств обработки, хранения и передачи информации, могущей быть преобразованной в*

форму, пригодную для однозначного восприятия человеком, и имеющей атрибуты для идентификации документа».

Статья 2 проекта Федерального закона «Об электронной цифровой подписи» [15]: — «*Электронное сообщение — информация, представленная в форме набора состояний элементов электронной вычислительной техники* (ЭВТ), *иных электронных средств обработки, хранения и передачи информации, могущей быть преобразованной в форму, пригодную для однозначного восприятия человеком, и имеющей атрибуты для идентификации документа*».

«*Электронный документ — электронное сообщение, имеющее реквизиты для идентификации его как документа*».

Статья 4 проекта Федерального закона «Об электронном документе» [20]: — «*Электронный документ представляет собой зафиксированную на материальном носителе информацию в виде набора символов, звукозаписи или изображения, предназначенную для передачи во времени и пространстве с использованием средств ВТ и электросвязи в целях хранения и общественного использования*».

Статья 5 проекта: — «*ЭлД должен быть представленным в форме, понятной для восприятия человеком*».

Действующий закон Республики Беларусь «Об электронном документе» [33]: — «*Электронный документ — информация, зафиксированная на машинном носителе и соответствующая требованиям, установленным настоящим законом*». ЭлД «*… должен быть представленным в форме, понятной для восприятия человеком*».

Закон Туркменистана «Об электронном документе» [36]: — «*… под электронным документом понимается информация, зафиксированная на машинном носителе, заверенная электронной цифровой подписью в соответствии с процедурой создания такой подписи*».

Проект закона Республики Казахстан «Об электронном документе и электронной цифровой подписи» [16]: — «*Электронное сообщение — информация, представленная в форме набора состояний элементов электронной вычислительной техники* (ЭВТ), *иных электронных средств обработки, хранения и передачи информации, которая может быть преобразована в форму, пригодную для однозначного восприятия человеком*». «*Электронный документ — электронное сообщение, содержащее электронную подпись участника системы электронного документооборота*».

Комментарий. Известный разнобой в определениях традиционного документа, конечно, нежелателен, но не критичен. Их применимость и адекватность проверена многолетней практикой. Иное дело — электронный документ, который воспринимается, преобразуется и обрабатывается компьютером, а не человеком. В определениях отчетливо просматривается тенденция на отождествление терминологии аналогового и электронного документооборота.

Даже из общих соображений симметрии (и, соответственно, асимметрии) это настораживает: механистическое распространение понятий за область определения ведет, как правило, к неудовлетворительным результатам. Ведь не требуется, чтобы аналоговый документ, например, денежная купюра, мог бы быть преобразован в форму, пригодную для однозначного восприятия компьютером. А вот для ЭлД требование однозначного восприятия человеком поставлено. С другой стороны, является ли обоснованием требования *фиксированности* ЭлД только то, что в течение всего жизненного цикла АнД зафиксирован на (бумажном) носителе?

В одних определениях прямо заявлено о фиксации ЭлД, в других, что одно и то же, только о его состоянии. Само слово «состояние» основано на понятии «стоять». В реальности состояние «элемента ЭВТ»

может меняться с частотой от нуля (домен дисковой памяти) до герц (изображение на мониторе) и далее до гигагерц (чип процессора). В какой момент времени фиксировать электронный документ, тем более — «набор состояний элементов ЭВТ», в определениях не говорится, равно как и не конкретизируются сами элементы, состояния которых есть форма представления сведения.

Все представленные определения ЭлД, по меньшей мере, неконструктивны, основаны на неверной в данном случае ассоциации с традиционным документом. Электронный документ существует в двух формах: пассивной — хранение; активной — передача и обработка. Нельзя говорить об обязательной фиксации или о состоянии электронного документа, если рассматривается активная форма его существования: тот промежуток времени, в течение которого он воспринимается, обрабатывается или передается.

Законодатель не заметил динамический характер активного существования ЭлД. Активизированный ЭлД индицируется во времени, а не в пространстве: чтобы переместить на малое расстояние ЭлД очень большого объема достаточно ничтожного сечения провода, но значительное время, пропорциональное объему документа. Для аналогового документа ситуация обратная: АнД индицируется в пространстве, а не во времени. Для того чтобы переместить на малое расстояние АнД очень большого объема достаточно ничтожного времени, но значительный объем пространства, пропорциональный объему документа.

С определенными натяжками требование закона можно применить к статическим реализациям ЭлД в режиме хранения на магнитном носителе: но и здесь координаты хранения неопределимы — где-то на диске. Если полагать, что «ЭлД зафиксирован на машинном носителе», то становится недопустимой стандартная операция «дефрагментация диска». А как

понимать дублирование файла на двух дискетах, его перезапись? Или передачу документа, файл которого был зафиксирован на диске одной машины, а теперь — на другой? Приходим к абсурду: фиксация (неизменность!) подразумевает изменение и в пространстве, и во времени.

Если определения законов положить в основу работы с ЭлД, то придется забыть об активизации документа, об его обработке, передаче, да и хранении — потому что запись представляет собой ни что иное, как *преобразование* динамической реализации в статическую. Строго говоря, предписания законов фактически исключают электронное взаимодействие.

Требование, что «… ЭлД должен быть представленным в форме, ***понятной*** *для восприятия человеком*» означает, что надо запретить использование ЭлД, по крайней мере, в коммерческой деятельности — наиболее привлекательной и экономически эффективной области применения электронных документов. Почти все документы, связанные с документальным оформлением финансовых потоков, технологически реализуются в форме, *недоступной* для восприятия человеком, даже при их непосредственной визуализации.

Так, электронное платежное поручение состоит из упорядоченной совокупности двоичных чисел. В нее входят: номер (шифр) типа финансового документа, числовой адрес банка, клиента, номер счета, сумма, валюта, одна или несколько электронных цифровых подписей (ЭЦП) и другие реквизиты. ЭЦП при визуализации представляется (в зависимости от стандарта) числом, включающим до 1000 двоичных разрядов, к тому же номера корреспондентского и банковского счетов требуют еще по 80 разрядов и т. д.

Визуализация электронного платежного поручения с ЭЦП даст несколько страниц, заполненных случайной, с позиций человека, совокупностью нулей и единиц. Можно преобразовать двоичный код в десятичный — тогда будет всего страница, заполненная цифрами. Но вряд

ли от этого облегчится восприятие. Если же буквально выполнять закон, т. е. формировать и обрабатывать электронное поручение в виде, подобном аналоговому, то его объем настолько возрастает за счет ненужной для ЭВМ информации (но нужной для восприятия человеком!), что обработка, передача, хранение ЭлД станет экономически нецелесообразной. Более того, так как визуализация ЭЦП (150-разрядное (!) десятичное число) не воспринимается человеком, то отсутствует один из важнейших «…реквизитов, позволяющих идентифицировать информацию», и, согласно определению, такое сообщение *не является* документом.

Можно, конечно, предположить, что закон предписывает возможность создания на основе исходного ЭлД и ряда других, хранящихся в ЭВМ, некоторого третьего электронного документа, который использовал бы часть информации исходного. Тогда, действительно, человек сможет воспринимать сформированный документ. Но это совсем другой документ, не исходный! ЭЦП нового документа должна отличаться от подписи исходного ЭлД.

В последнем по времени законе «Об электронной цифровой подписи» от 10.01.02 г. [26] понятие ЭлД определяется как «…*документ, в котором информация представлена в электронно-цифровой форме*». По сути, это тавтология: по видимому, «электронно» обозначает физическую природу носителя, а «цифровой» подразумевает логическую. Является ли изображение документа на экране монитора электронным документом? Электронная форма налицо, но цифровая как-то не замечается. Попробуйте найти электронную форму на перфокарте. Нет такой формы, следовательно, ЭлД нельзя записать в такой технологии, хранить, передавать, воспроизводить, использовать. А файл на диске памяти? Цифровая форма — записан двоичный файл, но вот электронная вызывает сомнение: поверхность диска эквивалентна листу бумаги, на котором невидимыми «чернилами» — ориентацией магнитных доменов, написан

двоичный текст. Кстати, обыкновенный печатный текст можно с полным правом отнести к цифровым формам отображения информации — если считать основание счисления равным числу букв в алфавите плюс количество цифр и знаков препинания.

Понятие «электронный документ» в принятых законах и разрабатываемых законопроектах не соответствует перспективе массового применения электронных документов в безлюдных технологиях электронного взаимодействия экономических субъектов.

1.1.3. Понятия «экземпляр», «подлинник», «копия», «юридическая сила» электронного документа

Разрешенные к применению формы аналоговых документов регистрируются и систематизируются Общероссийским классификатором управленческой документации (ОКУД) [37]. ОКУД является составной частью Единой системы классификации и кодирования технико-экономической и социальной информации и охватывает унифицированные системы документации и формы документов, разрешенных к применению в народном хозяйстве. Объектами классификации в ОКУД являются общероссийские (межотраслевые, межведомственные) унифицированные формы документов, утверждаемые министерствами (ведомствами) Российской Федерации.

Согласно Общероссийскому классификатору управленческой документации (ОКУД) [37] аналоговые документы по виду оформления различаются как:

ПОДЛИННИК — первый или единичный экземпляр документа;

ДУБЛИКАТ — повторный экземпляр подлинника документа, имеющий юридическую силу;

КОПИЯ — документ, полностью воспроизводящий информацию подлинного документа и все его внешние признаки или часть их, не имеющий юридической силы;

ЗАВЕРЕННАЯ КОПИЯ — копия документа, на которой в соответствии с установленным порядком проставляются реквизиты, придающие ей юридическую силу;

ВЫПИСКА — копия части документа, оформленная в установленном порядке.

В статье 9 проекта Федерального закона «Об электронном документе» [21] устанавливается: «*Все экземпляры ЭлД, подписанные одинаковым электронным аналогом подписи, имеют равное юридическое значение при условии подтверждения их подлинности в соответствии с требованиями настоящего Федерального закона*»[1].

Статья 11 проекта Федерального закона «Об электронной торговле» [19] гласит: «*Все экземпляры ЭлД, подписанные при помощи электронной цифровой подписи (ЭЦП), … являются подлинниками. Электронный документ не может иметь копий в электронном виде. …Копии ЭлД могут быть изготовлены (распечатаны) на бумажном носителе…* ».

В статье 9 закона «Об электронном документе» Республики Беларусь [33], в статье 7 закона «Об электронном документе» Туркменистана [36] утверждается: — «*Оригинал ЭлД существует только на машинном носителе. Все экземпляры ЭлД, зафиксированные на машинном носителе и идентичные один другому, являются оригиналами и имеют одинаковую юридическую силу*». В законах ничего не говорится об электронных копиях ЭлД, но явно допускается существование бумажных копий.

Комментарий. Если воспользоваться приведенной выше терминологией ОКУД, то возникают вопросы: что же такое подлинник?

[1] Термин «юридическое значение» неформален, слишком расплывчат. Скорее всего, разработчики говорят о «юридической силе» документа.

Все «экземпляры», или «первый или единичный экземпляр»? Отличаются ли между собой «подлинник» и «оригинал»? Являются ли два файла ЭлД в разных форматах (например, .doc, .txt или .arj) идентичными? Если отличаются, то какому из подлинников ЭлД можно придать статус оригинала, и чем оригинал-подлинник должен отличаться от просто подлинника? Если идентичны, то по каким признакам, ведь множества двоичных символов разных форматов явно отличны между собой? А если не идентичны, то чем один формат хуже другого?

Разработчики законов не дают определений понятий «экземпляр ЭлД», «подлинник ЭлД», «идентичные ЭлД», так что возможны, конечно, любые толкования. Но во всех приведенных предписаниях зафиксировано в явном виде существование нескольких экземпляров электронного документа, каждый из которых имеет юридическую силу оригинала. Не будем говорить, что по определению оригинал единственен и не может существовать в нескольких экземплярах. Важнее практические аспекты.

Например, *действующие* законы Республики Беларусь и Туркменистана предоставляют неограниченные возможности для обогащения. В соответствии с ними платежное поручение, записанное (для надежности) на нескольких дискетах или переданное несколько раз, дает формальное право на соответствующее число выплат. Действительно, если экземпляры идентичны, то имеют одинаковую юридическую силу. Раз первый по времени экземпляр поручения дает право на перечисление денег, то отказ для вновь поступившего, точно такого же, и имеющего такую же юридическую силу, противозаконен. Если бы закон выполнялся, то последствия очевидны.

Существование нескольких *оригиналов* электронной ведомости на выдачу зарплаты предполагает, что по каждой можно получить деньги, а признание оригиналом только одной означает, что в случае неудачной записи файла по другой (копии!? но ведь они неразличимы!) нельзя ничего

получить. Использование традиционной терминологии аналоговой среды применительно к электронному документу эквивалентно «очеловечиванию» машины и ведет к неустранимым парадоксам.

Операция копирования органически присуща электронной среде, более того, в определенном смысле это абсолютно точная операция, так что конкретизация копии — крайне сложная техническая задача. В огромном числе ситуаций, особенно в финансовой и коммерческой сфере, применяются документы однократного действия, например, то же самое платежное поручение. Здесь обязано выполняться требование единственности оригинала (подлинника) документа. В этих случаях невозможно соблюдать закон — считать каждый экземпляр подлинником. Необходимо нарушать закон, принятый на государственном уровне и подписанный Президентом страны.

В ст. 12 проекта Федерального закона «Об электронной торговле» [19] предписывается, что при сохранении (очевидно, в базах данных) «*…ЭлД должны сохранять формат, в котором они были сформированы, переданы или получены*». Чтобы не противоречить предыдущей статье 11 этого же законопроекта, запрещающей электронные копии ЭлД, остается предположить, что хранятся только подлинники документов. Законодатель не определяет понятия «формат ЭлД», так что приходится ступить на зыбкую тропу догадок.

Если «формат» подразумевает техническую реализацию ЭлД, то проект закона запрещает даже стандартные операции переформатирования файла, например, архивирование файла, и, наоборот, требует хранения массы избыточной «технологической информации». Достаточно напомнить, сколько раз меняется формат ЭлД при его «формировании, передаче, получении». Даже если допустить, что под «форматом» понимается визуальное отображение ЭлД, т. е. некоторый аналоговый документ, то и здесь хотя бы масштаб картинки выбирается произвольно.

Если же «формат» означает отсутствие дополнительных надписей на подлиннике, то закон запрещает любую модификацию ЭлД-оригинала, характеризующую его исполнение. Это в аналоговом документе любая надпись может рассматриваться как виза на оригинале и неразрывно связана с ним. В электронной среде любое изменение или дополнение ЭлД кардинально его меняет. Для ЭлД однократного действия, где оригинал необходимо должен «погашаться», чтобы исключить его повторное использование, и в таком виде храниться для отчетности, выполнение требований закона «Об электронной торговле» означает невозможность электронной торговли.

Цитированные законы и проекты явно или неявно не допускают наличие электронных копий ЭлД, но зато прямо говорят о возможности бумажных копий. Если понимать под «копией» приведенное выше определение ОКУД [37], то возникает естественный вопрос: какие «*внешние признаки ЭлД или часть их, воспроизводит*» бумажная копия ЭлД? Тем более странным выглядит предписание, что «*электронный документ не может иметь копий в электронном виде*». Тем самым предписывается хранить в составе ЭлД цифровую подпись автора на момент архивирования: документ с иной удостоверяющей подписью — это копия. А ведь согласно закону ЭлД «*не может иметь*» электронных копий! Придется забыть об архивировании ЭлД, даже если не обращать внимания на «*внешние признаки*» ЭлД и считать, что электронная копия полностью воспроизводит информацию подлинного документа.

В электронных финансовых документах значительный объем занимает электронная цифровая подпись (ЭЦП). Если это, например, платежный документ, содержащий несколько ЭЦП, то их объем может превышать 90% общего объема ЭлД. Подобные документы должны храниться длительное время. ЭЦП одного и того же юридического или физического лица неизбежно должна измениться за несколько лет, хотя бы

в силу прогресса в криптографии и вычислительной технике. Поэтому ЭЦП регистрируется на определенный период, после которого аннулируется, теряет свою практическую значимость, и может быть заменена на новую.

При запросе хранимого ЭлД из архива документ должен заверяться действующей в данный момент подписью владельца архива, не имеющей прямого отношения к автору документа. Архиватор должен гарантировать, что этот документ действительно был несколько лет назад подписан автором, чью ЭЦП, ныне аннулированную, архиватор обязан был проверить в момент архивирования. Если следовать положениям цитированных законов, то надо на порядок увеличивать объем архивов, время поиска и передачи, и т. д. И все это для того, чтобы сохранить устаревшую цифровую подпись, которую и проверить через несколько лет невозможно.

А что делать с электронными документами массового назначения (например, законами) при запросе из официального архива? Передать документ пользователю с ЭЦП Президента страны? По закону электронная копия не имеет права на существование, так что каждый желающий будет иметь в распоряжении документ с ЭЦП Президента. Любую ЭЦП можно дискредитировать, только это требует огромных ресурсов. Но ЭЦП Президента стоит очень дорого, затраты на ее дискредитацию могут и окупиться. А это уже прямая угроза информационной безопасности. Не проще ли предоставить *электронную копию* президентского ЭлД, заверенную действующей в данный момент подписью хранителя документа?

Вот к каким абсурдным с позиций здравого смысла следствиям ведет использование предписываемой законами терминологии. Законодатели «чувствуют», что ЭлД принципиально отличен от АнД, поэтому и предлагают рассматривать ЭлД как *множество* неразличимых объектов

(«экземпляров»), а не как *отдельный* объект, что характерно для АнД, но не «осознают» этого или боятся пойти против доминирующего толкования. Поэтому допускается множество оригиналов (подлинников, экземпляров), запрещаются электронные копии, переформатирование ЭлД, придается равная юридическая сила каждому «подлиннику, экземпляру» ЭлД.

Понятие «экземпляр» электронного документа необходимо конкретизировать. Является ли экземпляром ЭлД файл в оперативной памяти? или запись файла в ином формате? или заархивированный файл? или преобразование файла для его представления на экране монитора? или множество пакетов, на которые «разрезается» файл для его передачи, и т. д. и т. п.? А ведь все это — один и тот же электронный документ. Налицо неправомерное распространение понятий, эффективных в одной среде, на объекты другой, принципиально отличной среды.

1.1.4. Понятие «электронная цифровая подпись»

Для последующего анализа понятий, используемых в Федеральном законе «Об электронной цифровой подписи» [26], приведем известные определения в соответствии с международным стандартом ИСО/МЭК 14888-1-98 [29].

(*Электронная*) *цифровая подпись* (*digital signature*), *ЭЦП* — строка бит, полученная в результате процесса формирования подписи.

Процесс формирования ЭЦП (*signature process*) — совокупность двух последовательных преобразований: вычисление хэш-кода сообщения; выработка собственно ЭЦП на основе криптографического преобразования хэш-кода сообщения.

Хэш-код (hash-cod) — строка бит, являющаяся выходным результатом хэш-функции.

Хэш-функция (hash-function) — функция, отображающая строки бит в строку бит фиксированной длины, такая, что:

- по данному результату функции невозможно вычислить исходные данные, отображенные в этот результат;
- для заданных исходных данных трудно найти другие исходные данные, отображаемые с тем же результатом;
- для двух произвольных исходных данных трудно найти одинаковое отображение.

Ключ подписи (*signature key*) — элемент *тайных* данных, специфичный для объекта и используемый только данным объектом в процессе формирования ЭЦП (часто используются синонимы «личный ключ», «закрытый ключ», в ГОСТе Р 34.10.94 [38] написано «…элемент *секретных* данных»). В России секретность ассоциируется с государственной тайной, в таком случае *секретный* ключ должен храниться в соответствии с режимными требованиями. На самом же деле речь идет именно о *личной тайне* владельца ключа.

Ключ проверки (*verification key*) — элемент данных, математически связанный с ключом подписи объекта, и используемый проверяющей стороной в процессе проверки ЭЦП (используется также термин «открытый ключ»).

Теперь можно попытаться разобраться, о чем гласит Закон об ЭЦП [26]. Объект законодательства определен в статье 3 (абзац 3): — «*Электронная цифровая подпись — реквизит ЭлД, предназначенный для защиты данного ЭлД от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в ЭлД*».

Комментарий. Во-первых, цифровая подпись предназначена для *аутентификации* автора документа, но не для защиты документа от подделки. Конечно, при определенных условиях ЭЦП позволяет выявить

подделку, но тогда с таким же успехом и *отпечатки* пальцев можно определить как средство *защиты* от преступления. Документ, подписанный лицом, не имеющим на то полномочий, является недействительным. При этом цифровая подпись подлинная, однозначно определяет автора и, согласно Закону, защищает документ от подделки. Следовательно, если исходить из Закона, то документ подлинный.

Во-вторых, ЭЦП не является результатом «криптографического преобразования», а есть результат двух последовательных преобразований: *открытое и общедоступное* — вычисление хэш-кода информации; *криптографическое* — формирование собственно ЭЦП на основе хэш-кода. О хэшировании в Законе не говорится ни единого слова, в сертификате на подпись требования к хэшированию, судя по тексту Закона, не включаются.

Односторонние функции широко применяются в криптографии, но если называть хэширование криптографическим преобразованием, то тогда и сложение двух чисел по модулю третьего или перестановка чисел или возведение в степень являются криптографией. Можно допустить, что законодатели включают хэш-функцию в *средства* ЭЦП — «аппаратные и (или) программные средства, обеспечивающие создание и подтверждение ЭЦП, а также создание открытых и закрытых ключей» (Ст. 3). Следует ли в таком случае, что компьютер или клавиатура, или оперативная память — средства ЭЦП? Кто определяет водораздел?

Возникает пространство для субъективного толкования предписаний Закона. Если относить хэш-функцию к *криптографическим* средствам ЭЦП, то алгоритм хэширования можно задать принудительно, в том числе, можно заставить субъекта применять «плохую» хэш-функцию, секрет (изготовление двойника документа) которой известен компетентным организациям. Тогда никакая криптография при формировании собственно цифровой подписи от подделки не защитит. Аргументируя статьями

Закона, любой юрист может утверждать, что ЭлД с такой «плохой» хэш-функцией также является подлинным: его цифровая подпись удовлетворяет всем требованиям ст. 4-1 Закона, значит, искажения *отсутствуют*. С другой стороны, если считать, что хэш-функция не является средством ЭЦП, то ответственность за ее применение возлагается на отправителя документа, и претензии к центру, удостоверяющему цифровую подпись, не имеют правовой основы.

В-третьих, ЭЦП не позволяет «*идентифицировать владельца* подписи». Что такое идентификация? Отнесение одного из представленного множества объектов к некоторой категории. Идентифицировать владельца подписи — это опознать из шеренги людей того, кто подписал данный документ. Но на самом деле требуется «*привязать*» документ как объект к субъекту-автору, существующему независимо и вне документа, аутентифицировать документ.

Аутентификация документа — объективное подтверждение содержащейся в нем *идентифицирующей* информации. Понятия «идентификация (identification — отождествление)» и «аутентификация (authentification — достоверность)» близки; в аналоговой среде — среде приблизительной терминологии — обычно используется первое. В электронной среде, требующей однозначности, такое совмещение смыслов ведет к абсурдным результатам. Не случайно, что термин «аутентификация» стал широко использоваться именно в сфере электронного взаимодействия.

В-четвертых, ЭЦП не позволяет установить «*отсутствие искажения*» в ЭлД, а является *средством обнаружения* подделки документа. Подлинность ЭЦП говорит только о том, что возможные искажения не выявлены, вероятность «пропуска» подделки не равна нулю, хотя и очень мала. А вот если метод дискредитации ЭЦП известен, то подделка проста. Если у вас поддельный документ с подлинной цифровой

подписью, то судебное разбирательство невозможно: по закону в документе *отсутствуют* искажения, документ подлинный. Признать обратное — нарушить Закон.

В работе [39] рассмотрен случай, когда владелец, исходя из известных хэш-кодов *двух* различных сообщений, может рассчитать две пары (закрытый — открытый) ключей таким образом, что построенные на разных закрытых ключах ЭЦП этих *разных* сообщений будут *тождественны*. После этого владелец отказывается от подписанного им при помощи первого закрытого ключа сообщения, утверждая, что на самом деле он подписывал второе сообщение другим закрытым ключом. По закону ЭЦП «защищает от подделки» и подтверждает «отсутствие искажений», так что за «случайное» совпадение владелец не отвечает и требует соответствующих страховых выплат.

Статистическая значимость количества ошибок в столь важных позициях ответственных документов, разрабатываемых разными коллективами и в разных странах, исключает субъективные причины. Это не отдельные результаты, которые можно было бы объяснить субъективными причинами, неудачно выбранными словами для изложения в целом правильного положения: нечеткость (fuzzy) семантики языка позволяет «придраться» к любому определению. Это парадоксы в исходных понятиях, лежащие на поверхности. Только в цитированных документах можно указать помимо приведенных еще десяток неверных положений.

Системные положения существующих законов и разрабатываемых законопроектов не учитывают структурный сдвиг в электронном взаимодействии, обусловленный отказом от взгляда на ЭВМ как на «большую пишущую машинку». Еще некоторое время существующие нормативные материалы будут достаточно эффективны. Однако этот этап заканчивается, банковские технологии электронного взаимодействия уже

сейчас представляют собой фактически безлюдные технологии. Опыт последних 5—7 лет показывает, сколь быстро страна прошла путь к массовому применению ПЭВМ, а темпы информатизации все нарастают.

Законы необходимо отражают доминирующее в обществе представление об электронной информации. Менталитет меняется медленнее технологии, господствующие взгляды на электронный документ не соответствуют требованиям уже ближайшей перспективы. Становится очевидным, что в рамках традиционного описания информационного взаимодействия между мыслящими субъектами невозможно адекватное отображение процессов в электронной среде. Существующий подход, опирающийся на понятийную базу обмена информацией посредством традиционного (аналогового) документа, не соответствует требованиям современного, и тем более — будущих этапов развития электронного взаимодействия.

Необходимо исследование системных особенностей электронного документа, его отличий от традиционного, разработка новой вербальной модели электронного документа.

1.2. Существующие модели защиты электронной информации

1.2.1. Платформа анализа

Модель есть отображение качественных характеристик явлений мира объектов, описываемого *физическими* законами, в количественные показатели виртуального мира, описываемого *логическими* законами. Физические законы реальны, их действие проявляется непосредственно в форме состояния объектов реального мира. Логические законы виртуальны, их справедливость устанавливается на основе интерпретации количественных показателей, предсказанных моделированием, в качественные характеристики реального состояния объектов в точке

прогноза. Но раз есть интерпретация на выходе модели, то обязательно должна быть интерпретация и на входе.

Интерпретация на входе модели задается аксиоматикой моделирования — совокупностью взаимно *независимых* исходных утверждений, постулатов, правил, задающих процесс моделирования. Если аксиоматика, «вход» модели, адекватна физическому миру, то и результаты моделирования соответствуют практике: модель есть *однозначное* отображение входа на выход, в том смысле, что любое повторение моделирования с неизменными входными данными приведет к точно таким же результатам. В свою очередь, однозначность модели необходимо влечет конечность аксиоматической базы, иначе это означало бы возможность выполнения бесконечного числа независимых правил в течение конечного времени моделирования, что невозможно.

Таким образом, *бесконечность* качественных и количественных характеристик реальных явлений должна отображаться на входе модели в *конечную* аксиоматическую базу. Процесс перехода от бесконечности к конечности в общем случае принципиально не формализуется, иначе не существовало бы самого понятия бесконечности. Поэтому любая формальная модель необходимо должна включать в свой состав эвристический компонент — выделение конечного подмножества характеристик моделируемого явления и их интерпретацию в аксиоматическом виде. Это положение кажется очевидным, тем не менее, о нем часто забывают, опуская интерпретацию. Как правило, это проявляется в сочетании в модели строгих понятий математики с неформальными терминами, трактуемыми по умолчанию в достаточно широком диапазоне.

В сфере информационной безопасности должна существовать иерархическая *система* моделей различного уровня. При разработке моделей следует исходить из наличия *трех* кардинально различных сред

существования электронного документа: электронной, аналоговой, социальной. Можно наметить следующие уровни системы моделей: *информация, документ, отдельные механизмы защиты информации, защита среды существования, защита электронного взаимодействия*.

Модели информации должны базироваться на возможности *количественного* подхода к столь многообразному явлению как информация. Только тогда можно применять количественные оценки, только тогда можно говорить о цифровой информации, которая воспринимается неодушевленными объектами, инструментальными средствами вычислительной техники.

Модели документа основаны на признании его *социальным* явлением, существующим *только в рамках* общественной среды жизнедеятельности человека. Безразлично, традиционный или электронный документ, необходимыми условиями использования его в качестве информационного факта являются предусмотренные основания для возникновения, изменения, прекращения конкретных правоотношений между участниками информационного взаимодействия.

Только определив ЭлД, можно переходить к моделям отдельных механизмов защиты информации. В пассивном состоянии (хранение) ЭлД — это элемент пространства — *объект*, предмет. И с этой точки зрения подобен традиционному документу, «написанному» на поверхности «бумаги», ферромагнитной поверхности диска, невидимыми «чернилами», биполярной ориентацией магнитных доменов. В активном состоянии (обработка и передача) ЭлД — это *процесс*, развивающийся во времени.

1.2.2. Модели электронной информации

Модели цифровой информации опираются на ставшие уже классикой общеизвестные работы К. Шеннона [2, 40], показавшего возможность *количественного* подхода к информации. К каким парадоксам

в электронной среде приводит определение информации как сведения или знания показано выше. Сведение, знание — это сугубо индивидуализированные понятия, неотрывные от воспринимающего *субъекта*: для кого сведение, а для кого — пустой набор слов. Основная идея Шеннона заключается в *объективизации понятия* информации. Шеннон обезличил информацию, назвал информацией последовательность сигналов, бит и т. п. с заданной на ней вероятностной мерой.

Если вспомнить, что специализацией К. Шеннона была криптография (доклад «Математическая теория криптографии» был им сделан 01.09.45 г.), то подобный подход очевиден. Ведь зашифрованная информация, с позиций обычного человека, есть бессмысленный набор знаков, но никак не сведение или факт. Естественно, что «индивидуальность» множества в таком случае оказывается несущественным фактором, имеют место только абстрактные характеристики. Любая последовательность есть *упорядоченное* множество, тогда неизменность информации означает, что любые преобразования множества сохраняют отношение порядка, являются изоморфными.

Далее, используя чисто формальные математические преобразования, Шеннон приходит к понятиям энтропии, количества информации, совершенной секретности и прочим характеристикам, интерпретация которых имеет прикладное значение. Как правило, именно это ставят ему в заслугу, но исходные постулаты несопоставимо глубже. Электронное взаимодействие вышло на массовый уровень, и подавляющее большинство участников не способно адекватно воспринимать постулаты цифрового отображения информации, противоречащие всему их предыдущему жизненному опыту. В свою очередь, это ведет к поверхностному анализу процессов обеспечения информационной безопасности, не затрагивающему их глубинных основ.

1.2.3. Модели электронного документа

Федеральный закон «Об обязательном экземпляре документов» [24] гласит: «*Документ — материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования*».

Приведенное определение традиционного (аналогового) документа связывает в единое целое его пространственные (материальный объект), временные (передача, хранение во времени) и социальные (общественное использование) характеристики. Аналоговый документ практически постоянен во времени, поэтому можно говорить о *фиксированности* АнД. Документ индицируется как сосредоточенный в конечном объеме пространства и бесконечно малом интервале времени. Используемые способы отображения информации в АнД характеризуются жесткой связью с носителем (бумагой), так что допустимо интерпретировать АнД в течение всего жизненного цикла только как материальный объект.

Для электронного документа подобная абсолютизация неприемлема. В пассивном состоянии (хранение) ЭлД есть элемент пространства — *объект*, и с этой точки зрения подобен традиционному документу.

В активном состоянии (обработка и передача) ЭлД — *процесс*, здесь понятие фиксированности документа бессмысленно, процесс принципиально развивается во времени. Процесс в бесконечно малом интервале времени наблюдения не индицируется. В отличие от АнД, для индикации электронного документа как процесса необходим *конечный* период наблюдения, но достаточен *бесконечно малый* объема пространства: достаточен физический *контакт* с источником сигнала, а объем любого контакта практически равен нулю.

Но это не означает, что на практике используется единственный контакт, точка индикации ЭлД. Обычно требуется *конечное* число контактов, как-то распределенных в пространстве, разумеется, их суммарный объем все равно будет практически нулевым. Так как координаты возможных контактов известны лишь приближенно, в лучшем случае, с точностью до технического устройства, то нельзя ограничиться только *временной* составляющей ЭлД как процесса. Необходимо рассматривать и пространственный аспект ЭлД, ограничивающий зону возможных контактов. При защите информации, в частности, это приводит к задаче защиты электронной среды как совокупности инструментальных средств, хотя последние инвариантны, *не зависят* от собственно информации.

И, наконец, социальный аспект электронного документа, обусловленный его использованием для регулирования общественных отношений между участниками информационного взаимодействия. Документ, в отличие от сообщения, представляет собой *социальное* явление, существующее только в рамках общественной среды жизнедеятельности человека. Применение ЭлД в документообороте означает его использование в качестве сообщения о возникновении *юридического* факта — предусмотренного в законе основания для возникновения, изменения, прекращения конкретных правоотношений между участниками взаимодействия.

Социальная среда предъявляет требования, отсутствующие в электронной среде, важнейшие из которых: аутентификация участников взаимодействия, доступность пользователю, конфиденциальность сообщения. Причем выполнение этих требований должно не только обеспечиваться «по умолчанию», но и подтверждаться наличием тех или иных, индицируемых в явном виде, статусных атрибутов электронного документа. Аналогично, показания свидетелей некоторого события

становятся *юридическим фактом* и могут быть использованы в судебной практике только при *явном* подтверждении предписанной законами технологии и процедур сбора, регистрации, верификации, оглашения и т. д.

В настоящее время обмен информацией в электронном виде технически и технологически не представляет принципиальных трудностей. На рынке предлагается множество сопоставимых по качеству инструментальных и программных средств, позволяющих реализовать электронное взаимодействие между удаленными пользователями как в режиме «on-line», так и в режиме «off-line». Однако ситуация кардинально меняется, как только выдвигается требование *документированности* электронного взаимодействия. Необходимо придать *юридический* статус некоторому виртуальному объекту, не индицируемому органами чувств человека в пассивной фазе (хранение) жизненного цикла, не фиксированному в активной фазе (обработка и передача), меняющемуся в любой из моментов наблюдения.

Удовлетворительные модели электронного документа, отражающие отмеченные аспекты, в доступной литературе найти не удалось. На современном этапе развития электронного взаимодействия разработка подобных комплексных моделей является крайне актуальной задачей.

1.2.4. Модели механизмов защиты информации

Приведем аннотационное описание наиболее часто цитируемых моделей, в том числе: дискреционного, мандатного, дискретного доступа; синхронных и асинхронных распределенных систем; трансформации прав доступа; элементарной защиты; гарантированно защищенной системы; модель изолированной программной среды; субъектно-объектная модель; и др.

1. Модель дискреционного доступа [42]. В рамках модели контролируется доступ субъектов к объектам. Для каждой пары субъект-объект устанавливаются операции доступа (READ, WRITE и др.). Контроль доступа осуществляется посредством механизма, который предусматривает возможность санкционированного изменения правил разграничения доступа. Право изменять правила предоставляется выделенным субъектам. В моделях дискретного доступа [43–45] рассматриваются отдельные механизмы распространения доступа субъектов к объектам.
2. Модель мандатного управления доступом Белла—Лападула [43, 46, 47]. Формально записана в терминах теории отношений. Описывает механизм доступа к ресурсам системы, при этом для управления доступом используется матрица контроля доступа. В рамках модели рассматриваются простейшие операции доступа субъектов к объектам READ и WRITE, на которые накладываются ограничения. Множества субъектов и объектов упорядочены в соответствии с их уровнем безопасности. Состояние системы изменяется согласно правилам трансформации состояний. Во множестве субъектов могут присутствовать доверенные субъекты, которые не подчиняются ограничениям на операции READ и WRITE. В таком случае модель носит название модели доверенных субъектов [43].
3. Модели распределенных систем (синхронные и асинхронные) [43]. В рамках модели субъекты выполняются на нескольких устройствах обработки. В рамках модели рассматриваются операции доступа субъектов к объектам READ и WRITE, которые могут быть удаленными, что может вызвать противоречия в модели Белла—Лападула.

   В рамках асинхронной модели в один момент времени несколько субъектов могут получить доступ к нескольким объектам. Переход

системы из одного состояния в состояние в один момент времени может осуществляться под воздействием более, чем одного субъекта.

4. Модель безопасности военной системы передачи данных (MMS-модель) [43, 46, 48]. Формально записана в терминах теории множеств. Субъекты могут выполнять специализированные операции над объектами сложной структуры. В модели присутствует администратор безопасности для управления доступом к данным и устройством глобальной сети передачи данных. При этом для управления доступом используются матрицы контроля доступа. В рамках модели используются операции доступа субъектов к объектам READ, WRITE, CREATE, DELETE, операции над объектами специфической структуры, а также могут появляться операции, направленные на специфическую обработку информации. Состояние системы изменяется с помощью функции трансформации.
5. Модель трансформации прав доступа [46]. Формально записана в терминах теории множеств. В рамках модели субъекту в данный момент времени предоставляется только одно право доступа. Для управления доступом применяются функции трансформации прав доступа. Механизм изменения состояния системы основывается на применении функций трансформации состояний.
6. Схематическая модель [46, 50]. Формально записана в терминах теории множеств и теории предикатов. Для управления доступом используется матрица доступа со строгой типизацией ресурсов. Для изменения прав доступа применяется аппарат копирования меток доступа.
7. Иерархическая модель [46, 51]. Формально записана в терминах теории предикатов. Описывает управление доступом для параллельных вычислений, при этом управление доступом основывается на вычислении предикатов.

8. Модель безопасных спецификаций [46, 52]. Формально описана в аксиоматике Хоара. Определяет количество информации, необходимое для раскрытия системы защиты в целом. Управление доступом осуществляется на основе классификации пользователей. Понятие механизма изменения состояния не применяется.
9. Модель информационных потоков [46, 53]. Формально записана в терминах теории множеств. В модели присутствуют объекты и атрибуты, что позволяет определить информационные потоки. Управление доступом осуществляется на основе атрибутов объекта. Изменением состояния является изменение соотношения между объектами и атрибутами.
10. Вероятностные модели [43]. В модели присутствуют субъекты, объекты и их вероятностные характеристики. В рамках модели рассматриваются операции доступа субъектов к объектам READ и WRITE. Операции доступа также имеют вероятностные характеристики.
11. Модель элементарной защиты [54]. Предмет защиты помещен в замкнутую и однородную защищенную оболочку, называемую преградой. Информация со временем начинает устаревать, т.е. цена ее уменьшается. За условие достаточности защиты принимается превышение затрат времени на преодоление преграды нарушителем над временем жизни информации. Вводятся вероятность непреодоления преграды нарушителем $P_{\text{сзи}}$, вероятность обхода преграды нарушителем $P_{\text{обх}}$ и вероятность преодоления преграды нарушителем за время, меньшее времени жизни информации $P_{\text{хр}}$. Для введенной модели нарушителя показано, что $P_{\text{сзи}} = \min [(1 - P_{\text{обх}}), (1 - P_{\text{хр}})]$, что является иллюстрацией принципа слабейшего звена. Развитие модели учитывает вероятность отказа системы и вероятность обнаружения и блокировки действий нарушителя.

12. Модель системы безопасности с полным перекрытием [44, 55]. Отмечается, что система безопасности должна иметь по крайней мере одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему. Модель описана в терминах теории графов. Степень обеспечения безопасности системы можно измерить, используя лингвистические переменные [56, 57]. В базовой системе рассматривается набор защищаемых объектов, набор угроз, набор средств безопасности, набор уязвимых мест, набор барьеров.
13. Модель гарантированно защищенной системы обработки информации [6]. В рамках модели функционирование системы описывается последовательностью доступов субъектов к объектам. Множество субъектов является подмножеством множества объектов. Из множества объектов выделено множество общих ресурсов системы, доступы к которым не могут привести к утечке информации. Все остальные объекты системы являются порожденными пользователями, каждый пользователь принадлежит множеству порожденных им объектов. При условии, что в системе существует механизм, который для каждого объекта устанавливает породившего его пользователя; что субъекты имеют доступ только общим ресурсам системы и к объектам, порожденным ими, и при отсутствии обходных путей политики безопасности, модель гарантирует невозможность утечки информации и выполнение политики безопасности.
14. Субъектно-объектная модель [58, 59]. В рамках модели все вопросы безопасности описываются доступами субъектов к объектам. Выделено множество объектов и множество субъектов. Субъекты порождаются только активными компонентами (субъектами) из объектов. С каждым субъектом связан (ассоциирован) некоторый объект (объекты), т.е. состояние объекта влияет на состояние субъекта. В модели присутствует специализированный субъект — монитор безопасности

субъектов (МБС), который контролирует порождение субъектов. Показана необходимость создания и поддержки изолированной программной среды.

Из упомянутых моделей наибольший интерес представляют дискреционные и мандатные механизмы разграничения доступа (как наиболее распространенные), модель гарантированно защищенной системы (в силу гарантированности) и субъектно-объектная модель (рассматривающая не только доступы, но и среду, в которой они совершаются). В [43] предлагаются следующие исходные понятия для моделирования защиты информации.

Сущность, под которой понимается любая составляющая компьютерной системы.

С*убъект* — активная сущность, которая может инициировать запросы ресурсов и использовать их для выполнения каких-либо вычислительных заданий.

Объект — пассивная сущность, используемая для хранения и получения информации.

Доступ — взаимодействие между объектом и субъектом, в результате которого происходит перенос информации между ними.

Взаимодействие происходит при исполнении субъектами *операций*.

Существуют *две фундаментальные операции*:

- *чтение* — перенос информации от объекта к субъекту;
- *запись* — перенос информации от субъекта к объекту.

Утверждается, что данные операции являются минимально необходимым базисом для описания моделей, описывающих защищенные системы.

Уровень безопасности определяется как иерархический атрибут. Каждый составляющий компонент системы ассоциирован с уровнем безопасности.

Для представления уровней безопасности введено:

- L — множество уровней безопасности;
- символы « < », « ≤ », « > », « ≥ » — описывающие иерархические отношения между элементами множества L.

Комментарий. Даже из столь краткого представления моделей очевидным становится, что они базируются на феноменологическом описании процессов и объектов электронной среды. Исходные понятия даются на эвристическом уровне: есть нечто, понимаемое по умолчанию как электронная информация, или как электронный документ, или как операция, или как процесс в электронной среде и т. д. В формальную модель вводятся полуопределенные, расплывчатые понятия социальной среды: «сущность», «субъект», «объект», «доступ», «право», «полномочие», и т. п. При таком представлении интерпретация моделей и результатов не абсолютна (однозначна), а относительна (многозначна) — допускает широкий диапазон толкований, зависящий от квалификации и подготовки пользователя.

Например, утверждение «2×2 = 4» — абсолютно, не зависит от квалификации воспринимающего субъекта. А теперь рассмотрим понятие «несанкционированный доступ — НСД» с позиций математика, программиста и юриста. Для математика несанкционированный доступ *непонятен* в принципе: либо путь (доступ) из одной вершины графа в другую существует, либо нет, и никаких санкций для этого не требуется. Для программиста НСД означает существование алгоритма инициализации протокола доступа, *отличающегося* от приведенного в руководстве или инструкции пользователю. Для юриста НСД означает запуск предусмотренного *стандартного* протокола доступа лицом, не имеющим на то административных полномочий.

По существу наблюдается та же самая картина, с которой мы столкнулись в разделе 1.1 при анализе понятийной базы законов в сфере

электронного взаимодействия. Только в законах применяется бытовой сленг, а при описании моделей — профессиональный жаргон разработчиков инструментальных средств, разбавленный поверхностными знаниями математики. Для простых моделей подобное допустимо, конкретная интерпретация понятий возможна по умолчанию. Но с ростом сложности моделируемого явления адекватность теряется, и правильно истолковать результаты моделирования может только разработчик, зачастую вкладывающий в трактовку понятий свое индивидуальное видение, в корне отличающееся от канонического определения.

Аннотированные модели априорно рассчитаны на применение специалистами с квалификацией, позволяющей им более-менее однозначно трактовать тот сленг, на котором описана модель, понять, что же именно модель уточняет. Преимущество компактности описания достигается за счет узости применения, фактически уточняются свойства и требования к *отдельным механизмам* защиты информации от несанкционированного доступа (НСД) — основному виду угроз информационной безопасности. До начала моделирования специалист уже представляет конечный результат, его цель — только конкретизация количественного измерения результата. Это эффективно на начальных этапах электронного взаимодействия, когда средства защиты и нападения достаточно очевидны.

С качественным ростом сложности вычислительных систем, появлением все более и более изощренных методов и способов атак, эффективность подобных моделей падает. «Смешивание» в единой модели качественно отличающихся сторон электронного взаимодействия — требований аналоговой, цифровой и социальной среды существования документа, — допустимо только на примитивном уровне описания. Мы приходим к тому же самому положению, что и в приведенном анализе понятийной базы вербальных моделей ЭлД.

Существующие модели защиты информации имеют экстенсивный характер (обо всем понемножку), что в перспективе должно негативно сказаться на эффективности их применения. Необходима специализация моделей, учитывающая качественное различие свойств и требований к электронному документу при его переходе на этапах жизненного цикла из одной среды существования в другую.

Чтобы не быть голословными, рассмотрим далее более детально модели информационной безопасности, получившие наибольшее распространение в настоящее время.

1.2.5. Модели разграниченного доступа

Известные модели разграничения доступа, построенные по принципу предоставления прав, делятся на два основных типа: модели дискреционного и мандатного доступа. Предлагаются [60–62] различные отечественные реализации дискреционного механизма, отличающиеся, в первую очередь, составом набора общих прав.

В СЗИ НСД «Dallas Lock» [60] неявно используются атрибуты $R_D = \{Y, N\}$, где Y — право полного доступа субъекта к объекту (на чтение, запись, модификацию и т. д.); N — отсутствие такого права. В соответствии с этим каждому субъекту-пользователю ставится в соответствие либо список разрешенных объектов, либо список запрещенных объектов.

В СЗИ НСД «Secret Net» [61] набор применяемых атрибутов шире, а именно $R_S = \{R, W, X\}$, где R — право (разрешение) на чтение; W — право на модификацию; X — право на запуск задачи.

Наиболее полный набор общих прав используется в СЗИ НСД «Аккорд» [62] и включает $R_A = \{R, W, C, D, N, V, O, M, E, G, X\}$, где:

- R — разрешение на открытие файлов только для чтения;

- W — разрешение на открытие файлов только для записи;
- C — разрешение на создание файлов на диске;
- D — разрешение на удаление файлов;
- N — разрешение на переименование файлов;
- V — видимость файлов;
- O — эмуляция разрешения на запись информации в файл;
- M — разрешение на создание каталогов на диске;
- E — разрешение на удаление каталогов на диске;
- G — разрешение перехода в этот каталог;
- X — разрешение на запуск программ.

Заметим, что наборы атрибутов R_S и R_A близки к атрибутам, применяемым в ОС UNIX и NetWare соответственно.

Опуская особенности реализации, рассмотрим некоторые возможности применения различных наборов атрибутов для описания политик информационной безопасности.

Пусть набор атрибутов — $R_D = \{Y,\ N\}$. Предположим, что в системе действуют два пользователя U_1 и U_2. Каждый пользователь имеет право полного доступа Y к некоторому множеству объектов, иными словами, для пользователя U_1 определен список разрешенных объектов $\{O_{11}, \mathbf{K}, O_{1n_1}\} = \{O_{1i}\}_{i=1}^{n_1}$, обозначим его $\mathbf{O_1}$. Для пользователя U_2 соответственно определен список разрешенных объектов $\{O_{21}, \mathbf{K}, O_{2n_2}\} = \{O_{2i}\}_{i=1}^{n_2}$, обозначим его $\mathbf{O_2}$.

В случае, когда $O_1 \mathbf{I} O_2 \neq \varnothing$*, т. е. когда существует хотя бы один объект, который содержится в списке разрешенных объектов как для пользователя* U_1*, так и для пользователя* U_2*, возможна утечка информации.*

Покажем это. Пусть существует: $O \in \mathbf{O}_1$ и $O \in \mathbf{O}_2$, т. е. $\mathbf{O}_1 \mathbf{I} \mathbf{O}_2 = O$. Представим список разрешенных объектов пользователя U_1 следующим образом: $\mathbf{O}_1 = O \mathbf{U} \mathbf{O}_1'$. Предположим, что пользователя U_2 интересуют данные, хранящиеся в объекте $O' \in O_1'$. При этом пользователь U_1 помещает в объект O данные из объекта O', а пользователь U_2, в свою очередь, может прочитать эти данные, так как $O \in \mathbf{O}_2$. Таким образом, пользователь U_2 получает доступ к информации, хранящейся в объекте $O' \in \mathbf{O}_1'$, к которому U_2 не имеет права доступа, т. е. происходит утечка информации.

Для описанного состава атрибутов утечка информации возможна в любом случае, когда $\mathbf{O}_1 \mathbf{I} \mathbf{O}_2 \neq \varnothing$, т. е. существует только одна выполнимая политика безопасности, а именно: списки разрешенных пользователям объектов не имеют общих элементов. Ясно, что это очень сильное ограничение, тем более что и его недостаточно. Действительно, если право полного доступа подразумевает возможность переименования объекта, то возможны и другие каналы утечки, аналогичные описанным.

Комментарий. С субъективной точки зрения результат понятен специалисту, соответствует реальности, но, в определенном смысле, он не вытекает из модели и даже ей противоречит. Причина — некорректное описание модели: смешение чисто формальной терминологии математики с бытовым и профессиональным сленгом. Из определений «вдруг» оказывается, что общее право — это не одно право (например, чтения), а несколько прав (в том числе, право копирования, право изменения текста). Да и само понятие «утечка информации» не определено. На таком поле понятий можно сконструировать любое предложение, в том числе, и противоположное. Например,

В случае, когда $\mathbf{O}_1 \mathbf{I} \mathbf{O}_2 = Æ$, *т. е. когда* ***не*** *существует ни одного объекта, который содержался бы в списке разрешенных объектов как для*

пользователя U_1 так и для пользователя U_2, возможна утечка информации.

Для обоснования достаточно подразумевать (но умолчать в утверждении!), что существует третий пользователь U_3, для которого определен список разрешенных объектов, имеющий непустое пересечение со списками для пользователя U_1 и для пользователя U_2. Как и раньше, здесь кое-что (наличие третьего пользователя) недоговорено. Но если умолчание разрешено для первого положения, то почему недопустимо для второго?

Понятия: «определен», «право», «доступ» или, еще более расплывчатого — «*полный* доступ», в модели определены некорректно. «Право» есть характеристика субъекта, «доступ» есть операция на множестве из субъектов и объектов, это абсолютно разные математические характеристики. Для существования права не нужны объекты, а вот *операция* доступа без наличия объектов немыслима. Что отличает «полный доступ» от просто «доступа»? Существует ли «неполный доступ», и что это такое? Разумеется, из контекста понятно, о чем на самом деле идет речь, но в *модели* подобное недопустимо.

«Здравый смысл» — это не доказательство, а только предпосылка существования доказательства. Разумеется, на начальных этапах развития проблематики защиты информации подобные неформальные модели допустимы, а зачастую — и необходимы. Только на основе таких моделей можно перейти к обобщению частных результатов и их формализации.

Перейдем к дальнейшему обзору. Рассмотрим теперь набор атрибутов $R_S = \{R, W, X\}$. Этот набор шире R_D. Действительно, атрибуты из R_D могут быть описаны атрибутами из R_S, а именно: $Y = \{R, W, X\}$; $N = \{-, -, -\}$. Обратное — невозможно.

Предположим, что в системе действуют два пользователя U_1 и U_2: пользователь U_1 имеет права доступа $\{R, W\}$ к объекту O_1; пользователь U_2 имеет право доступа $\{R\}$к объекту O_2. Предположим, что пользователя U_2 интересуют данные, хранящиеся в объекте O_1. При этом пользователь U_1, пользуясь имеющимся у него правом W на модификацию объекта O_1, может переименовать его в O_2. Пользователь U_2, в свою очередь, пользуясь имеющимися у него правами $\{R\}$ на объект O_2, получает доступ к данным, которые содержались в объекте O_1, т. е. происходит утечка информации. При этом ни пользователь U_1, ни пользователь U_2 не нарушают политики безопасности. Таким образом, для данного состава атрибутов утечка информации возможна в том случае, если хотя бы один из пользователей имеет право доступа $\{W\}$ к защищаемому объекту.

Это также очень сильное ограничение, и в этой связи возможности разграничения доступа, предоставляемые данным набором атрибутов, обычно усиливаются дополнительными механизмами.

Атрибуты из R_S, в свою очередь, могут быть описаны атрибутами из R_A, а именно: $\{R\}_{R_S} = \{R\}_{R_A}$; $\{W\}_{R_S} = \{R, W, C, D, N\}_{R_A}$; $\{X\}_{R_S} = \{X\}_{R_A}$. Обратное невозможно.

Комментарий принципиально не отличается от приведенного при анализе атрибутов $R_D = \{Y, N\}$. Просто здесь выше размерность, шире набор прав, более громоздкие взаимосвязи, вводится некая иерархия прав и доступов. Но, как и ранее, основополагающие для моделей понятия «право», «доступ», «утечка», «модификация» и др. не формализуются, о содержательной сущности приходится только догадываться, опираясь на сопровождающий контекст и семантику обозначения терминов.

1.2.6. Модели дискреционного доступа

Для каждой из реализаций моделей дискреционного доступа фундаментальным является вопрос, является ли безопасной та или иная начальная конфигурация, т. е. возможна или нет утечка некоторого права. Другими словами, может ли пользователь при некоторых условиях получить доступ к объекту, если в начальном состоянии возможность такого доступа не предусмотрена (не установлено соответствующее право). В общем случае ответ на этот вопрос дается в модели дискреционного доступа с позиций распространения прав доступа.

Рассмотрим дискретную модель разграничения доступа, приведенную в [43], как модель распространения прав доступа. Система защиты представляется в виде некоторого декартова произведения множеств, составными частями которых являются составные части системы защиты: субъекты, объекты, уровни доступа, операции и т. д. В качестве математического аппарата выбран аппарат теории множеств.

Типичная модель системы защиты состоит из следующих частей:

1. $R=\{r_1,\mathbf{K},r_n\}$ — конечный набор общих прав;

2. S_0 — конечный набор исходных субъектов, O_0 — конечный набор исходных объектов, где $S_0 \subseteq O_0$;

3. C — конечный набор команд формы $a(X_1,\mathbf{K}X_n)$, где a — имя, $X_1,\mathbf{K}X_n$ — формальные параметры, указывающие на объекты;

4. J — интерпретация для команд, такая, что J отображает C в последовательность элементарных операций.

Элементарными операциями являются (r — общее право; s — имя субъекта; o — имя объекта):

- ввести право r в (s, o);
- удалить право r из (s, o);
- создать субъект s;

- создать объект *o*;
- разрушить субъект *s;*
- разрушить объект *o*.

5. Условия для команд. Условие *C* — отображение элементов набора команд в конечный набор прав.

Право — это тройка (r, s, o), где $r \in R$, а s и o — формальные параметры.

6. *P* — матрица доступов со строкой для каждого субъекта из S и столбцом для каждого объекта из *O*.

Комментарий. Итак, по п. 2 «типичной модели системы защиты» субъект непременно есть объект, но объект не обязательно является субъектом. Возникает естественный вопрос, а чем отличаются «*объект-субъект*» от «*объект-несубъект*», ведь это исходные понятия модели? Какой из объектов понимается в паре (s, o), который «*несубъект*», или который «*субъект*»? Если по определению право есть тройка (r, s, o), то, даже формально, как можно «удалить право из двойки (s, o)? Конечно, можно догадаться, что именно подразумевается. Но только догадаться! Кстати, а чем отличается «*общее* право» от просто «*право*»? Определено, что общее право есть r (одиночка, но не тройка!), а просто право есть тройка (r, s, o). Что такое «команда»? Если α — имя, то не являются ли «формальные параметры X_i, указывающие на объекты» также именами? Что такое «разрушить объект», «разрушить субъект»? И поскольку «субъекты есть подмножество объектов, $S_0 \subseteq O_0$», то означает ли разрушение субъекта, что одновременно разрушается объект?

Далее. Если слова в п. 4 действительно означают *элементарные* операции (на множестве O_0, на множестве S_0, на множестве $O_0 \setminus S_0$), то эти операции должны быть определены и, в силу элементарности, взаимно независимы. Опять-таки можно только догадываться, о чем идет речь.

Нечеткость и ошибочность исходных положений неминуемо должны отражаться и на следствиях.

Далее приводятся определения из модели дискреционного доступа.

Определение 1. Для заданной системы защиты команда $a(X_1,\mathbf{K}X_n)$ может привести к утечке общего права r, если ее интерпретация содержит некоторую операцию вида «ввести r в (s, o) для некоторых $o\in O$ и $s\in S$».

Определение 2. Для заданной системы защиты и права r начальная конфигурация $(s_0\, o_0\, p_0)$ является безопасной для r в этой системе, если не существует конфигурации $(s\, o\, p)$, такой что $(s_0\, o_0\, p_0)$ ведет к $(s\, o\, p)$, и существует команда $a(X_1,\mathbf{K}X_n)$, условия которой удовлетворяются в $(s\, o\, p)$, и которая для некоторых реальных параметров дает утечку права r через команду «ввести r в (s,o) для некоторых $o\in O$ и $s\in S$», причем s и o существуют во время команды «ввести» и для них r не находится в $p[s,o]$, где $p[s,o]$ — элемент матрицы доступа P.

Для моделей, построенных на основе дискретной защиты, доказана следующая

Теорема. Не существует алгоритма, который может решить для произвольной дискретной защиты и общего права r, является или нет заданная исходная конфигурация безопасной.

Комментарий. Что такое «заданная система защиты»? Хотя бы, как можно задать «систему защиты»? Учитывая, что к тому же и понятия «конфигурация», «интерпретация» не определены, говорить о справедливости теоремы бессмысленно. Тем более что попутно возникла еще одна тройка (s, o, p), отличная от тройки (r, s, o).

1.2.7. Модели мандатного доступа

Классической моделью, лежащей в основе построения многих систем мандатного доступа является модель Белла и Лападула (БЛМ), описание которой приводится далее по [6] на основе [63].

Классы объектов предполагаются неизменными. Определены конечные множества ***S***, ***O***, ***R***, ***L***.

S — множество субъектов системы;

O — множество объектов, не являющихся субъектами;

R — множество прав доступа; ***R*** = {*read (r), write(w), execute (e), append (a)*};

L — уровни секретности.

(Скорее всего, как и в предыдущей модели, субъекты обязательно являются объектами, но обратное не всегда справедливо. Если — да, то зачем выделять как множество ***S*** некоторое подмножество ***O***? Если субъект не является объектом, то зачем описывать множество ***O***?)

Множество ***V*** состояний системы определяется произведением множеств: $\boldsymbol{V}=\boldsymbol{B}\times\boldsymbol{M}\times\boldsymbol{F}\times\boldsymbol{H}$, где сомножители определяются следующим образом:

B — множество текущих доступов и есть подмножество множества подмножеств произведения $\boldsymbol{S}\times\boldsymbol{O}\times\boldsymbol{R}$. Множество подмножеств обозначается $P(\boldsymbol{S}\times\boldsymbol{O}\times\boldsymbol{R})$; элементы множества ***B*** обозначаются *b*, и они представляют в текущий момент *t* графы текущего доступа (в каждый момент субъект может иметь только один вид доступа к данному объекту).

(Если ***B*** есть подмножество, то чем это подмножество отличается от других подмножеств $\boldsymbol{S}\times\boldsymbol{O}\times\boldsymbol{R}$, и причем здесь графы, а, например, не матрицы? Кстати, матрица разрешенных доступов далее вводится. Откуда появляется «граф текущего доступа», и что такое «доступ» в терминологии теории графов, или теории матриц?).

M — матрица разрешенных доступов, $\boldsymbol{M}=|M_{ij}|$, $M_{ij}\subseteq\boldsymbol{R}$.

F — подмножество множества $\boldsymbol{L}^{s}\times\boldsymbol{L}^{s}\times\boldsymbol{L}^{o}$, где каждый элемент $f=(f_s, f_0, f_c), f\in\boldsymbol{F}$, - вектор, который состоит из трех компонентов, каждый из которых тоже вектор (или отображение):

f_s — уровень допуска субъектов (это некоторое отображение *f:* ***S***->***L***);

f_o — уровень секретности объектов (это некоторое отображение *f:* ***O***->***L***);

f_c — текущий уровень секретности субъектов (это тоже некоторое отображение *f:* ***S***->***L***).

Элементы подмножества ***F***, которые допущены для определения состояния, должны удовлетворять соотношению:

$$\forall S\in \boldsymbol{S}\ \ f_s(S)\geq f_c(S)$$

H — текущий уровень иерархии объектов, в [63] этот уровень не изменяется, совпадает с f_o и далее не рассматривается.

Элементы множества ***V*** состояний обозначаются через *v*.

Определены множества: ***Q*** — запросов в систему; ***D*** — решений по поводу запросов (***D*** = {yes, no, error}).

Множество ***W*** действий системы определено как $\boldsymbol{W}\subseteq\boldsymbol{Q}\times\boldsymbol{D}\times\boldsymbol{V}\times\boldsymbol{V}=\{(q,d,v_2,v_1)\}$.

Каждое действие системы *(q, d, v_2, v_1)* имеет следующий смысл: если система находилась в данный момент в состоянии v_1, поступил запрос *q*, то принято решение *d* и система перешла в состояние v_2.

Пусть ***T*** — множество значений времени (***T***=**N** — множество натуральных чисел).

Определен набор из трех функций (*x, y, z*). *x:* ***T***->***Q***, *y:* ***T***->***D***, *z:* ***T***->***V***, и обозначены множества таких функций ***X***, ***Y***, ***Z*** соответственно.

Рассмотрим $\boldsymbol{X}\times\boldsymbol{Y}\times\boldsymbol{Z}$ и определим понятие системы в БЛМ.

Определение 1. Системой $\mathrm{å}(\boldsymbol{Q}, \boldsymbol{D}, \boldsymbol{W}, z_0)$ называется подмножество $\boldsymbol{X} \times \boldsymbol{Y} \times \boldsymbol{Z}$ такое, что $(x, y, z) \hat{I} \mathrm{å}(\boldsymbol{Q}, \boldsymbol{D}, \boldsymbol{W}, z_0) \hat{U} \left(x_t, y_t, z_t, z_{t-1}\right) \hat{I} \boldsymbol{W}$ для каждого значения $t \hat{I} \boldsymbol{T}$, где z_0 — начальное состояние системы.

Определение 2. Каждый набор $(x, y, z) \hat{I} \mathrm{å}(\boldsymbol{Q}, \boldsymbol{D}, \boldsymbol{W}, z_0)$ называется реализацией системы.

Определение 3. Если (x, y, z) — реализация системы, то каждая четверка $\left(x_t, y_t, z_t, z_{t-1}\right)$ называется действием системы.

Определение 4. Тройка $(S, O, X) \hat{I} \boldsymbol{S} \times \boldsymbol{O} \times \boldsymbol{R}$ удовлетворяет свойству простой секретности (ss-свойство) относительно f, если $X=execute$, или $X=append$, или, если $X=read$ и $f_s(S) \geq f_o(O)$, или $X=write$ и $f_s(S) \geq f_0(O)$.

Определение 5. Состояние $v=(b, \boldsymbol{M}, f, h)$ обладает ss-свойством, если для каждого элемента $(S,O,X) \hat{I} \boldsymbol{B}$ этот элемент обладает ss-свойством относительно f.

Определение 6. Состояние $v=(b, \boldsymbol{M}, f, h)$ обладает *-свойством, если для каждого $(S, O, X) \hat{I} \boldsymbol{B}$ при $X=write$ текущий уровень субъекта $f_c(S)$ равен уровню объекта $f_0(O)$, или при $X=read$ $f_c(S) \geq f_0(O)$, или при $X=append$ $f_o(O) \geq f_c(S)$.

Определение 7. Состояние обладает *-свойством относительно множества субъектов $\boldsymbol{S'}$, $\boldsymbol{S'} \hat{I} \boldsymbol{S}$, если оно выполняется для всех троек (S, O, X) таких, что $S \hat{I} \boldsymbol{S'}$

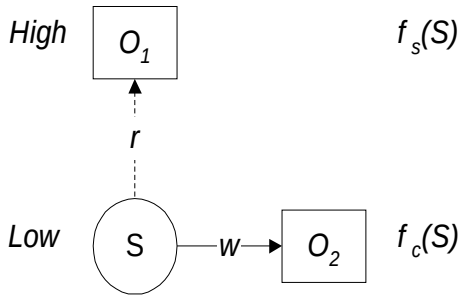
Определение 8. Субъекты из множества $\boldsymbol{S} \backslash \boldsymbol{S'}$ называются доверенными.

Определение 9. Состояние $v=(b, \boldsymbol{M}, f, h)$ обладает ds -свойством, если $"(S, O, X) \hat{I} b => X \hat{I} m_{so}$, где $\boldsymbol{M}=||m_{so}||$- матрица доступа состояния v, т. е. $\forall$ доступы из множества текущих доступов для $S \in \boldsymbol{S}$ и $O \in \boldsymbol{O}$ находятся в матрице разрешенных доступов.

Определение 10. Состояние $v = (b, M, f, h)$ называется безопасным, если оно обладает одновременно ss-свойством, *- свойством относительно S' и ds-свойством.

Из определения ss-свойства следует, что в безопасном состоянии возможно чтение вниз, кроме того, ss-свойство определяет ограничение на возможность модификации, которое связано с *write*: $fs(S) \geq fo(O)$.

Объясним *-свойство. Если субъект может понизить свой текущий допуск до $f_c(S)=f_0(O)$, то, согласно *-свойству, он может писать в объект. При этом он не может читать объекты на более высоких уровнях, хотя допуск $f_s(S)$ ему это может позволить. Тем самым исключается возможный канал утечки:



Таким образом, при записи информационный поток опять не может быть направлен вниз. Исключение возможно только для доверенных субъектов, которым разрешено строить информационный поток вниз. При этом доверенность субъекта означает безопасность такого потока вниз (поэтому эти потоки считаются разрешенными).

Для того чтобы доказать, что любой поток на траектории вычислительной системы разрешен, достаточно показать, что, выходя из безопасного состояния и следуя допустимым действиям, мы опять приходим в безопасное состояние, тем самым любая реализация процесса будет безопасной.

Определение 11. Реализация *(x, y, z)* системы $\mathring{a}(\boldsymbol{Q}, \boldsymbol{D}, \boldsymbol{W}, z)$ обладает ss-свойством (*-свойством, ds- свойством), если в последовательности (z_0, z_1,.....) каждое состояние z_n обладает ss-свойством (*-свойством, ds-свойством).

Определение 12. Система обладает ss-свойством (соответственно, *-свойством, ds-свойством), если каждая ее реализация обладает ss-свойством (соответственно, *-свойством, ds-свойством).

Определение 13. Система называется безопасной, если она обладает одновременно ss-свойством, *-свойством и ds - свойством.

Теорема A1. $\mathring{a}(\boldsymbol{Q}, \boldsymbol{D}, \boldsymbol{W}, z_0)$ обладает ss -свойством для любого начального z_0, которое обладает ss-свойством тогда и только тогда, когда $\boldsymbol{W}$ удовлетворяет следующим условиям для каждого действия (q, d, (b*, $\boldsymbol{M}$*, f*, h*), (b, $\boldsymbol{M}$, f, h)):

(1) $\forall(S, 0, X) \in b^* |$ b обладает ss-свойством относительно f*;

(2) если $(S, O, X) \in b$ и не обладает ss-свойством относительно f*, то $(S, O, X) \notin b^*$.

Теорема A2. Система $\mathring{a}(\boldsymbol{Q}, \boldsymbol{D}, \boldsymbol{W}, z_0)$ обладает *- свойством относительно $\boldsymbol{S'}$ для любого начального состояния z_0, обладающего *-свойством относительно $\boldsymbol{S}$' тогда и только тогда, когда $\boldsymbol{W}$ удовлетворяет следующим условиям для каждого действия (q, d, (b*, $\boldsymbol{M}$*,f*, h*), (b, $\boldsymbol{M}$, f, h)):

(I) $\forall S \in \boldsymbol{S'}$, $\forall(S, O, X) \in b^* \setminus b$ обладает *-свойством относительно f*;

(II) $\forall S \in \boldsymbol{S'}$, $\forall(S, O, X) \in b$ и (S, O, X) не обладает *-свойством относительно f*, то $(S, O, X) \notin b^*$.

Теорема A3. Система $\mathring{a}(\boldsymbol{Q}, \boldsymbol{D}, \boldsymbol{W}, z_0)$ обладает ds-свойством тогда и только тогда, когда для любого начального состояния, обладающего ds-свойством, $\boldsymbol{W}$ удовлетворяет следующим условиям для любого действия (q, d, (b*, $\boldsymbol{M}$*,f*, h*), (b, $\boldsymbol{M}$, f, h)):

(I) $(S, O, X) \in b^* | b$, то $X \in m_{so}^*$,

(II) $(S, O, X) \in b^* | b, X \notin m_{so}^*$, то $(S, 0, X) \notin b^*$.

Теорема (Basic Security Theorem). Система $\Sigma(Q, D, W, z_0)$ — безопасная тогда и только тогда, когда z_0 — безопасное состояние и W удовлетворяет условиям теорем А1, А2, А3 для каждого действия.

Таким образом, построенная модель является безопасной, но при этом на рассматриваемую систему накладывается ряд достаточно жестких ограничений.

Как отмечено выше, *-свойство позволяет субъекту понижать его текущий допуск до уровня секретности объекта и при этом не дает возможности читать из объекта с более высоким уровнем секретности.

Предположим, что субъект S получил доступ *read* к объекту O_1, считал интересующую его информацию, затем понизил свой текущий уровень допуска и, получив доступ *write* к объекту O_2, произвел в него запись данных, прочитанных из O_1.

Приведенный пример демонстрирует возможный канал утечки, при том, что не происходит нарушения политики безопасности, т. е. все действия субъекта являются правомерными.

Исключить ситуацию, подобную данной, возможно только лишь при условии, что система не обладает памятью. Данное ограничение, очевидно, является неприменимым к наиболее часто используемым системам.

Рассмотренное конечное множество прав доступа $R = \{read, write, execute, append\}$ обеспечивает работу системы, а именно, доступ субъектов к интересующим их объектам, только на прикладном уровне.

Комментарий. Трудно сказать что-либо определенное о модели БЛМ, кроме того, что она базируется на огромном количестве плохо определенных и/или заданных множеств. Достаточно только перечислить часть из них: $S, O, R, L, B, M, F, H, V = B \times M \times F \times H, B = S \times O \times R, X, Y, Z,$

$X \times Y \times Z$, L^s, L^c, L^o, $F = L^s \times L^c \times L^o$, Q, D, T, N, $W = Q \times D \times V \times V$, (Q, D, W, z) и др. А ведь сюда еще надо добавить векторные пространства с неопределенными свойствами, матрицы с незаданными операциями, функции, которые не функции, права и доступы с неясной математической интерпретацией.

Коль скоро в рассмотрении вводятся вектора, то, по крайней мере, должно быть задано начало координат, определены характеризующие векторное пространство F операции умножения вектора на скаляр и векторного сложения. Кроме того, множество F должно быть кольцом (замкнутым относительно операций пересечения и симметрической разности). Создается впечатление, что указанные положения авторам модели незнакомы. Во всяком случае, их выполнение крайне неочевидно. Огромная загадка, что же такое множество матриц разрешенных доступов $M=|M_{ij}|$, $M_{ij} \subseteq R$? Судя по тексту, это множество не только состоит всего из одной матрицы, но одновременно является подмножеством множества «прав доступа» $R = \{read\ (r),\ write(w),\ execute\ (e),\ append\ (a)\}$. Всякая функция есть отображение, но далеко не всякое отображение есть функция, для этого отображение должно быть определено на множестве чисел, но не на множестве элементов произвольной природы, в частности, множестве операций.

В модели надо определить математически, а что же именно защищается, выделить участников доступа, математическую сущность права, операции и т. п. Возможны две формы отображения электронной информации: статическое в аналоговом виде — в устройствах памяти, динамическое в цифровом виде — как процесс преобразования. Модель сводит динамику к статике, рассматривая «объекты-субъекты» и «объекты-несубъекты». Наверное, как можно догадаться, это активизированный файл и файл в памяти. Отсюда автоматически вытекает, что рассматриваемая модель априорно слишком схематична. Это все равно,

как изучать поведение функции только по ее значениям, отбрасывая понятия производных, интеграла и т. д. Можно, но не эффективно.

Жизненный цикл электронного документа протекает в трех средах: социальной (права), аналоговой (память), электронной (процесс). Существуют, по меньшей мере, два класса требований к защите документа: технологические — например, обеспечение доступности и целостности ЭлД; и социальные — конфиденциальность, секретность, обеспечение аутентификации ЭлД. Если при анализе первых достаточно рассматривать только электронную среду, то для исследования последних необходимо кардинально изменить модель, вводя мыслящего субъекта, т. е. качественно изменяя среду моделирования. Вместо этого в модели БЛМ вводится неопределенное «право доступа», маскируемое совместным использованием несовместимых языков описания: с одной стороны — «читать», «писать», «добавить», «уничтожить»; с другой стороны, язык математики — «декартово произведение множеств», «множество всех подмножеств», «векторное пространство», «граф текущего доступа», «функция».

Известно, что из «белого шума» можно выделить любую последовательность. Точно так же, из белого шума терминологии модели можно получить любое правильное заключение. Но можно — и неправильное, если заранее ответ неизвестен. Скорее всего, цитированная базовая теорема безопасности правильно определяет *достаточные* условия безопасности, но являются ли эти условия *необходимыми* — уже не очевидно.

1.2.8. Модель гарантированно защищенной системы обработки информации

В [6] определена модель ∑ системы, которая оперирует с ценной информацией. Согласно модели, время дискретно и принимает значения из множества N={l, 2, ... }. Информация в системе ∑, включая описание самой системы, представима в форме слов некоторого гипотетического языка ***Я*** над некоторым конечным алфавитом А.

Объект в ∑ — это конечное множество слов из ***Я***, состояние объекта — выделенное слово из множества, определяющего этот объект. С понятием объекта связано агрегирование информации в ∑ и о ∑.

Приведены следующие примеры объектов:

- объектом является принтер, который можно рассматривать как автомат с конечным множеством состояний, а эти состояния — суть слова языка ***Я;***
- объект — файл; множество слов, которые могут быть записаны в файле, является конечным и определяет объект, а состояния объекта — это текущая запись в файле, которая тоже является словом в языке ***Я***.

Вся информация о ∑ в данный момент может быть представлена в виде состояний конечного множества объектов. Считается, что состояние системы ∑ — это набор состояний ее объектов.

Объекты могут создаваться и уничтожаться, поэтому можно говорить о множестве объектов системы ∑ в момент ***t,*** которое обозначается O_t, $|O_t|<¥$. Для каждого $t Î N$ в O_t выделено подмножество S_t субъектов: $S_t \in O_t$. Любой субъект $S \in S_t$ есть описание некоторого преобразования информации в системе ∑. Каждый субъект может находиться в двух состояниях: в форме описания, в котором субъект называется неактивизированным, и в форме (процесс), в которой субъект называется активизированным.

Активизировать субъект может только другой активизированный субъект. Для каждого $t \hat{I} N$ на множестве $\mathbf{S_t}$ определяется орграф Γ_t, где S_1 и S_2 из $\mathbf{S_t}$ соединены дугой S_1->S_2 тогда и только тогда, когда в случае активизации S_1 возможна активизация S_2. Если субъект S — такой, что для каждого Γ_t в вершину S не входят дуги, то такой субъект называется пользователем. Предполагается, что в системе S всего два пользователя: U_1 и U_2. Пользователи считаются активизированными по определению и могут активизировать другие субъекты. Если в любой момент t в графе Γ_t в вершину S не входят дуги и не выходят дуги, то такие субъекты исключаются из рассмотрения. Введено обозначение: $S_1 \xrightarrow{a} S_2 \;\; S_1, S_2 \in \boldsymbol{S_t}$, процедуры активизации процессом S_1 субъекта S_2.

Далее в рамках модели делаются следующие предположения:

Предположение 1. Если субъект S активизирован в момент t, то существует единственный активизированный субъект S' в $\boldsymbol{S_t}$, который активизировал S. В момент t=0 активизированы только пользователи.

Лемма 1. Если в данный момент t активизирован субъект S, то существует единственный пользователь U, от имени которого активизирован субъект S, то есть существует цепочка $U \xrightarrow{a} S_1 \xrightarrow{a} S_2 \xrightarrow{a} \mathbf{L} \xrightarrow{a} S_k \xrightarrow{a} S$.

Предположение 1 требует единственности идентификации субъектов. Далее предполагается, что каждый объект в системе имеет уникальное имя.

Кроме активизации в системе $\sum$ существуют и другие виды доступа активизированных субъектов к объектам.

Введено множество всех видов доступов $\boldsymbol{R}$, $|\boldsymbol{R}| < \infty$. Если p Í $\boldsymbol{R}$, то множество доступов p активизированного субъекта S к объекту O обозначится через $S \xrightarrow{p} O$. Если в некоторый промежуток времени $[t, t+k]$ реализована последовательность доступов

$U \xrightarrow{a} S_1 \xrightarrow{a} S_2 \xrightarrow{a} \mathbf{L} \xrightarrow{a} S_k \xrightarrow{p} S$, то считается, что произошел доступ $S \xrightarrow{p} {}^{*}O$ от имени субъекта *S* к объекту *O*.

При этом не имеет значения, какую задачу решает система ∑, а лишь моделируется функционирование системы последовательностью доступов.

Предположение 2. Функционирование системы ∑ описывается последовательностью доступов множеств субъектов к множествам объектов в каждый момент времени $t \hat{I} \boldsymbol{N}$.

Описанный выше орграф Γ_t обобщается путем добавления дуг *S->O*, обозначающих возможность любого доступа субъекта *S* к объекту *O* в момент *t*, в случае активизации *S*.

Введено обозначение: $\boldsymbol{D_t(S)} = \{O \mid S \text{ --}>{}^{*}O$ в момент $t\}$, где *S->*O* означает возможность осуществления цепочки доступов $S->S_1->S_2->\ldots S_k->O$ (возможность доступа к *O* от имени *S*). Тогда для любого $t \hat{I} \boldsymbol{N}$ в системе определены $\boldsymbol{D_t(U_1)}$ и $\boldsymbol{D_t(U_2)}$.

Считается, что $\boldsymbol{D} = \boldsymbol{D_t(U_1)} Ç \boldsymbol{D_t(U_2)}$ фиксировано для всех *t*, $\boldsymbol{O_t} = \boldsymbol{D_t(U_1)} È \boldsymbol{D_t(U_2)}$, в начальный момент $t = 0$: $\boldsymbol{O_0} = \{U1,U2\} È \boldsymbol{D}$

Определение 1. Множество объектов ***D*** называется общими ресурсами системы.

Средствами из ***D*** пользователь может создавать объекты и уничтожать объекты, не принадлежащие ***D***. Создание и уничтожение каких-либо объектов является доступом в ***R*** к некоторым объектам из ***O*** (и к уничтожаемым объектам).

Из объектов системы ∑ построена некоторая подсистема, которая реализует доступы. Любое обращение субъекта *S* за доступом *p* к объекту *O* в эту подсистему начинается с запроса, который обозначается $S \xrightarrow{p?} O$.

При порождении объекта субъект S обращается к соответствующей процедуре, в результате которой создается объект с уникальным именем. Тогда в силу леммы 1, существует единственный пользователь, от имени

которого активизирован субъект, создавший этот объект, т. е. соответствующий пользователь породил данный объект.

Через $\boldsymbol{O_t(U)}$ обозначено множество объектов из $\boldsymbol{O_t}$, которые породил пользователь U. При этом считается, что $U \hat{I} \boldsymbol{O_t(U)}$.

В случае, если в $\boldsymbol{R}$ есть доступы *read* и *write*, рассматривается только опасность утечки информации через каналы по памяти, которые могут возникнуть при доступах к объектам. Таким каналом может быть следующая последовательность доступов при $s<t$:

$U_i \xrightarrow{w} O$ в момент s и $U_j \xrightarrow{r} O$ в момент t, $i \neq j$.

При определенных условиях может оказаться опасным доступ от имени пользователя:

$U_i \xrightarrow{w} {}^*O$ в момент s и $U_j \xrightarrow{r} {}^*O$ в момент t, $s<t$, $i \neq j$.

С некоторой избыточностью исчерпываются возможные каналы по памяти, если считать неблагоприятными какие-либо доступы $\boldsymbol{p_1, p_2 \subseteq R}$ вида

$$U_i \xrightarrow{p1} {}^*O,\ U_j \xrightarrow{p2} {}^*O,\ i \neq j, \qquad (1)$$

которые и считаются каналами утечки.

Предположение 3. Если $O \hat{I} \boldsymbol{D}$, то доступы в (1) при любых p_1 и p_2 не могут создать канал утечки.

Это значит, что предполагается невозможным отразить какую-либо ценную информацию в объектах общего доступа.

Тогда в (1) достаточно ограничиться объектами O, не лежащими в $\boldsymbol{D}$. Это значит, что в одном из доступов в (1) имеется $U_i \xrightarrow{pk} {}^*O$, где $O \hat{I} \boldsymbol{O_t}(U_j)$, $i \neq j$. Таким образом, в системе считаются неблагоприятными доступы вида:

$$\exists t, \exists p \subseteq \boldsymbol{R}, p \neq \varnothing, \exists U_i, \exists O \in \boldsymbol{O_t},$$

$$U_i \xrightarrow{p} {}^*O,\ O \hat{I} \boldsymbol{O_t}(U_j),\ i \neq j, \qquad (2)$$

то есть доступы от имени какого-либо пользователя к объекту, созданному другим пользователем. Такие доступы называются утечкой информации.

Предположение 4. Если некоторый субъект S, $S \hat{I} \boldsymbol{D}$, активизирован от имени пользователя U_i (т. е. $U_i \xrightarrow{a} {}^*S$), в свою очередь, субъекту S предоставлен в момент t доступ к объекту O, то либо $O \hat{I} \boldsymbol{D}$, либо $O \hat{I} \boldsymbol{O}_t(U_i)$, либо система прекращает работу и выключается.

Определена следующая политика безопасности (ПБ):

Если $S \xrightarrow{p?} O$, то при $S,O \in \boldsymbol{O}_t(U)$ доступ $S \xrightarrow{p} O$ разрешается, если $S \hat{I} \boldsymbol{O}_t(U_i)$, $O \hat{I} \boldsymbol{O}_t(U_j)$, $i \neq j$, то доступ $S \xrightarrow{p} O$ невозможен.

Теорема 1. Пусть в построенной системе выполняются предположения 1—4. Если все доступы осуществляются в соответствии с ПБ, то утечка информации (2) невозможна.

Далее построено удобное для реализации множество «услуг» более низкого уровня, поддерживающих ПБ. То есть определено множество условий, реализованных в системе Σ, таких, что можно доказать теорему о достаточности выполнения этих условий для выполнения правил ПБ.

Условие 1. (Идентификация и аутентификация). Если для любых $t \hat{I} \boldsymbol{N}$, $p \acute{I} \boldsymbol{R}$, S, $O \hat{I} \boldsymbol{O}_t$, $S \xrightarrow{p?} O$, то вычислены функции принадлежности S и O к множествам $\boldsymbol{O}_t(U_1)$, $\boldsymbol{O}_t(U_2)$, $\boldsymbol{D}$.

Условие 2. (Разрешительная подсистема). Если $S \hat{I} O_t(U_i)$, $O \hat{I} O_t(U_j)$ и $S \xrightarrow{p?} O$ в момент t, то из $i=j$ следует $S \xrightarrow{p} O$ и из $i \neq j$ следует $S \xrightarrow{p} O$ (не разрешается доступ).

Условие 3. (Отсутствие обходных путей политики безопасности). Для любых $t \hat{I} \boldsymbol{N}$, $p \acute{I} \boldsymbol{R}$, если субъект S, активизированный к моменту t, получил в момент t доступ $S \xrightarrow{p} O$, то в момент t произошел запрос на доступ $S \xrightarrow{p?} O$.

Теорема 2. Если в построенной системе ∑ выполняются предположения 1—4 и условия 1—3, то выполняется политика безопасности.

Комментарий. По сравнению с моделью Белла—Лападула сделан большой шаг вперед — фактически признана возможность *одновременного* существования информации (ЭлД) как в статической форме, так и в динамической. Более того, неявно и программные средства трактуются как информация — это концептуальный шаг вперед. Однако, словно испугавшись дальнейших выводов, авторы на этом и останавливаются. Более аккуратно и математическое описание модели, хотя уровень неряшливости все еще чрезмерен.

Как и ранее, не проводится четкого разграничения между пространством и временем, что могло бы существенно конкретизировать интерпретацию результатов модели. Модель в некотором смысле одномерна («в системе Σ всего два пользователя»), хотя среда существования документа в реальности много богаче, одновременно может происходить множество процессов в различных точках пространства. Модель априорно исходит из единственности траектории электронного документа. Крайне сильным является предположение о стерильности программной среды.

1.2.9. Субъектно-объектная модель (СО-модель). Изолированная программная среда

Дальнейшим шагом в развитии моделей стала субъектно-объектная модель, предложенная в [58, 59]. Модель произвольной АС рассматривается в виде конечного множества элементов. Указанное множество разделяется на два подмножества: множество объектов $O=\{O_i\}$ и множество субъектов $S=\{S_i\}$. Разделение АС на субъекты и

объекты предполагается априорным. Считается также, что существует априорный безошибочный критерий различения субъектов и объектов в АС (по свойству активности). Полагается, что в любой дискретный момент времени множество субъектов АС не пусто. Причем в противном случае соответствующие моменты времени исключаются из рассмотрения и рассматриваются отрезки с ненулевой мощностью множества субъектов.

Рассматривая вопросы безопасности информации в АС, говорится о защищенности системы как о состоянии, описанном в терминах модели АС. При этом понятие защищенности является для системы внешним, априорно заданным. Интегральной характеристикой, описывающей свойства защищаемой системы, является политика безопасности — качественное (или качественно-количественное описание) свойств защищенности, выраженное в терминах, описывающих систему.

Описание политики безопасности включает:

1. Множество возможных операций над объектами;

2. Для каждой пары «субъект, объект» (S_i, O_j) — назначение множества разрешенных операций, являющееся подмножеством всего множества возможных операций.

Сформулированы аксиомы защищенных АС, имеющие фундаментальное значение для всей теории информационной безопасности.

Аксиома 1. В защищенной АС всегда присутствует активный компонент (субъект), выполняющий контроль операций субъектов над объектами. Данный компонент фактически отвечает за реализацию некоторой политики безопасности.

Аксиома 2. Для выполнения в защищенной АС операций над объектами необходима дополнительная информация (и наличие содержащего ее объекта) о разрешенных и запрещенных операциях субъектов с объектами.

Аксиома 3. Все вопросы безопасности информации в АС описываются доступами субъектов к объектам.

Аксиома 4. Субъекты в АС могут быть порождены только активным компонентом (субъектами) из объектов.

Механизм порождения новых субъектов специфицируется следующим определением.

Определение 1. Объект O_i называется источником для субъекта S_m, если существует субъект S_j, в результате воздействия которого на объект O_i в АС возникает субъект S_m.

Вводится обозначение:

$Create(S_j,\ O_i) \rightarrow S_k$ — из объекта O_i порожден субъект S_k при активизирующем воздействии субъекта S_j. *Create* назовем операцией порождения субъектов.

Операция *Create* задает отображение декартова произведения множеств субъектов и объектов на объединение множества субъектов с пустым множеством: $Create: S \times O \rightarrow S \cup \{\varnothing\}$

Считается, что если $Create(S_j,\ O_i) \rightarrow \varnothing$, то порождение нового субъекта из объекта O_i при активизирующем воздействии S_j невозможно.

В рамках рассматриваемой модели в АС действует дискретное время и фактически новый субъект S_k порождается в момент времени $t+1$ относительно момента t, в который произошло воздействие порождающего субъекта на объект-источник.

С любым субъектом связан (или ассоциирован) некоторый объект (объекты), отображающий его состояние.

Определение 2. Объект O_i в момент времени t ассоциирован с субъектом S_m, если состояние объекта O_i повлияло на состояние субъекта в следующий момент времени (т.е. субъект S_m использует информацию, содержащуюся в объекте O_i).

Заметим также, что в рамках рассматриваемой модели в АС действует дискретное время и фактически новый субъект S_k порождается в момент времени t+1 относительно момента t, в который произошло воздействие порождающего субъекта на объект-источник.

Вводится обозначение «множество объектов $\{O_m\}_t$ ассоциировано с субъектом S_i в момент времени t»: $S_i(\{O_m\}_t)$.

Свойство субъекта «быть активным» реализуется и в возможности выполнения действия над объектами. При этом необходимо отметить, что пассивный статус объекта необходимо требует существования потоков информации от объекта к объекту (в противном случае невозможно говорить об изменении объектов), причем данный поток инициируется субъектом.

В рамках модели на временной оси выделяются несколько точек, имеющих принципиальное значение, а именно:

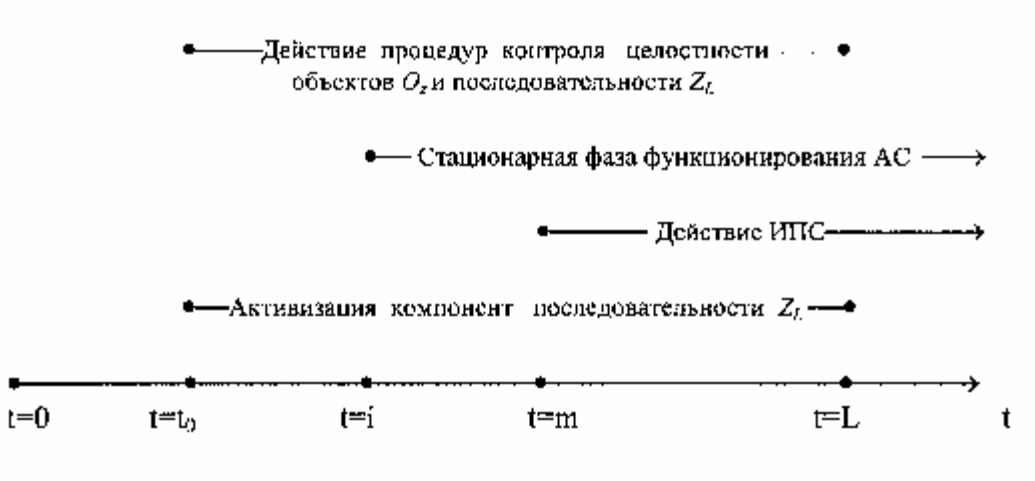
- t=0 — момент включения питания аппаратной части;
- $t=i$ — момент времени, в который наступает стационарная фаза функционирования АС;
- $t=m>i$ — момент времени, в который начинает действовать изолированная программная среда;
- $t=L$ — момент времени, когда завершена активизация всех компонентов АС, содержащихся в последовательности Z_L.

Отмечается, что субъект контроля неизменности объектов, входящих в процедуры активизации АС, и объектов, описывающих последовательность активизации компонентов, должен быть активен уже на этапе работы субъектов аппаратно-программного уровня, но его объект-источник технически не может быть проверен на неизменность. В связи с этим формулируется

Аксиома 5. Генерация ИПС (изолированной программной среды) рассматривается в условиях неизменности конфигурации тех субъектов

АС, которые активизируются до старта процедур контроля целостности объектов O_Z и последовательности Z_L. Неизменность данных субъектов обеспечивается внешними по отношению к самой АС методами и средствами. При анализе или синтезе защитных механизмов свойства указанных субъектов являются априорно заданными.

С учетом аксиомы 5 схематическое представление этапов функционирования АС принимает следующий вид:



Комментарий. В СО-модели сделан по сравнению с другими моделями значительный шаг вперед, так как рассмотрены механизмы и методы создания ИПС как безопасных начальных состояний. Действительно, в условия всех основных моделей входит некоторое безопасное начальное состояние, но в рамках моделей не рассматриваются конструктивные механизмы его достижения.

СО-модель отвечает на этот вопрос, дополняя, а не отвергая другие модели. Формируется иерархия моделей, где выделяются этапы генерации ИПС, поддержка ИПС и разграничение доступа как с помощью мандатных, так и дискреционных механизмов.

При этом СО-модели присущ и ряд серьезных недостатков. Так, например, очень сильным представляется требование аксиомы 5.

Действительно, невыполнение требований не позволит создать изолированную программную среду (ИПС), а как их реализовать, и что вообще означает «внешние априорно заданные средства», какими они должны быть?

В ряде позиций ограниченность как СО-модели, так и других связана также и с некоторыми упрощениями, не всегда обоснованными. Так, в СО-модели отмечается, что «все вопросы безопасности в АС описываются доступами субъектов к объектам» (аксиома 3). Такая формулировка вызывает серьезные вопросы — например, разве не связаны с безопасностью состав и структура системы?

С общих позиций, разделение множества элементов АС на два подмножества, объектов и субъектов, выглядит искусственным, что влечет массу дополнительных определений и ограничений, в частности, порождение объекта из субъекта и наоборот, ассоциирование объекта и субъекта, и др. На наш взгляд, существенно упростило бы модель принятие постулата, что любой элемент АС может находиться в двух состояниях: пассивном, тогда это состояние называется «объектом», и активном — тогда называется «субъектом». Ведь все программные средства хранятся в памяти, инициализация переводит их в активную форму. С другой стороны, преобразование информации ЭлД есть процесс.

Это позволило бы унифицировать операции преобразования. Примерно также расширение множества целых чисел на все рациональные числа позволяет допустить все арифметические операции, включая деление.

1.3. Выводы

1. Опубликованные в открытой печати законы и разрабатываемые законопроекты государственного уровня в сфере электронного

взаимодействия разрабатываются квалифицированными коллективами, проходят многократные обсуждения и экспертизу. Совокупность таких документов является представительной выборкой для определения доминирующего представления об электронной информации и электронном документе. Выполненный анализ позволил установить значительное число неточностей и парадоксов в исходных понятиях и определениях этих документов с точки зрения электронного взаимодействия и, соответственно, вытекающих отсюда предписаний и нормативов. Статистическая значимость количества ошибок в столь важных позициях ответственных документов, разрабатываемых разными коллективами и в разных странах, исключает субъективные причины.

2. Причина ошибок в исследованных документах — игнорирование кардинального, системного, отличия электронной, цифровой среды информационного взаимодействия от традиционной, аналоговой.

В технологиях обмена информацией происходит системный сдвиг, переход на более высокую ступень абстрактного отображения — документ, который раньше был прерогативой человека, теряет субъективизм, становится безличным, в каком-то смысле не зависящим от воли и сознания субъектов. Аналогия между традиционной (текст на бумаге) и электронной технологией отображения документа оправдана, только если компьютер используется как «большая пишущая машинка». Но уже сейчас, тем более в перспективе, такое использование компьютера — скорее исключение, чем правило. Существующий подход, опирающийся на понятийную базу обмена информацией посредством традиционного (аналогового) документа, не соответствует требованиям современного, а тем более — следующих этапов развития электронного взаимодействия.

Необходимо исследование системных особенностей электронного документа, его отличий от традиционного, разработка новой вербальной модели электронного документа.

3. Анализ наиболее распространенных моделей защиты информации показывает, что в понятийной базе моделей наблюдается та же самая картина, что и в понятийной базе законов в сфере электронного взаимодействия. Если в законопроектах делается попытка описания на языке неквалифицированного пользователя, то при описании моделей используется профессиональный жаргон рядового программиста с неглубокими знаниями математики. Модели базируются на феноменологическом описании процессов и объектов электронной среды. Исходные понятия даются на эвристическом уровне: есть нечто, понимаемое по умолчанию как электронная информация, как электронный документ, как операция, как процесс в электронной среде и т. п. В формальную модель вводятся полуопределенные, расплывчатые понятия социальной среды: «сущность», «субъект», «объект», «доступ», «право», «полномочие» и т. п. Одновременно используются строгие понятия математики: множество, декартово произведение множеств, векторное пространство, граф, матрица, отображение, функция и т. д. Причем анализ показывает, что подразумеваемые свойства таких математических объектов зачастую не имеют ничего общего с их классическим пониманием.

4. При таком представлении моделей интерпретация результатов не абсолютна (однозначна), а относительна (многозначна) — допускает широкий диапазон толкований, зависящих от квалификации и подготовки пользователя. Для простых моделей подобное допустимо, интерпретация понятий возможна по умолчанию. Но с ростом сложности моделируемого явления адекватность теряется, возникает неоднозначность в интерпретации. Правильно истолковать результаты моделирования может

только разработчик, вкладывающий в трактовку понятий свое индивидуальное видение, иногда противоположное написанному.

Тем не менее, модели следует оценить как весьма полезные на «ранних» этапах развития информационного обмена в электронной форме, когда все своеобразие взаимодействия описывается фразой «как обычно, только на экране монитора». В такой ситуации интерпретация «по умолчанию» оказывается эффективной. Существующие модели защиты информации имеют экстенсивный характер (обо всем понемножку), что в перспективе должно негативно сказаться на их применении. Необходима специализация моделей, учитывающая качественное различие свойств и требований к электронному документу при его переходе из одной среды существования в другую.

5. Любая формальная модель необходимо должна включать в свой состав эвристический компонент — выделение конечного подмножества характеристик моделируемого явления и их интерпретацию в аксиоматическом виде. Бесконечность качественных и количественных характеристик реальных явлений должна отображаться на входе модели в конечную аксиоматическую базу. Процесс перехода от бесконечности к конечности в общем случае эвристичен. Это положение очевидно, тем не менее, в рассмотренных моделях опускают интерпретацию, сочетая строгие понятия математики с неформальными бытовыми понятиями.

Отсутствие системного понимания электронного взаимодействия приводит к «выдергиванию» и абсолютизации отдельных состояний ЭлД на протяжении его жизненного цикла. Жизненный цикл документа проходит в трех средах — аналоговой, цифровой, социальной. Аксиоматика моделирования должна отображать на границах (интерфейсах) сред существования документа доминирующие характеристики столь качественно отличных явлений как социальная среда — общество, аналоговая среда — материальные объекты и предметы,

электронная среда — логические процессы. Необходимо учитывать существование ЭлД в виде объекта (в памяти) и в виде процесса (обработка и передача).

6. Требуется формализовать наличие мыслящих субъектов: аутентификация, конфиденциальность документа обусловлены только присутствием человека, социальной средой, в среде неодушевленных объектов эти понятия бессмысленны. Необходима иерархия моделей, позволяющая обосновать преобразование требований, предъявляемых социальной средой к защите информационного взаимодействия, в требования к аналоговой среде существования документа и далее — к электронной среде.

Короткий срок развития защиты информации как отдельной дисциплины не позволяет говорить о сколько-нибудь завершенной системе. Даже на низких уровнях иерархии имеется множество различных, несовместимых подходов и направлений моделирования. Как и должно быть, теория не успевает за технологическими достижениями. Попытка сведения в единой модели всех аспектов защиты информации априорно должна вести к крайне схематичным результатам.

Можно наметить следующие уровни иерархической системы моделей*: информация, документ, отдельные механизмы защиты информации, защита среды существования, защита электронного взаимодействия*.

7. Модели цифровой информации должны базироваться на ставших уже классикой общеизвестных работах К. Шеннона, показавшего возможность *количественного* подхода к столь качественно многообразному явлению, как информация. Основная идея Шеннона заключается в *объективизации понятия* информации. Только тогда можно применять количественные оценки, только тогда можно говорить о

цифровой информации, которая *воспринимается* неодушевленными объектами, инструментальными средствами вычислительной техники.

Удовлетворительные модели электронного документа, отражающие отмеченные аспекты, в доступной литературе найти не удалось. На современном этапе развития электронного взаимодействия разработка подобных комплексных моделей является крайне актуальной задачей.

8. Рассмотренные модели уточняют свойства и требования к *отдельным механизмам* защиты информации от несанкционированного доступа. Модели рассчитаны на применение специалистами с квалификацией, позволяющей им более-менее однозначно трактовать тот сленг, на котором описана модель, понять, что же именно модель уточняет. Указанные недостатки непринципиальны, и при грамотной обработке изложения могут быть устранены. Преимущество компактности описания здесь достигается за счет узости применения. До начала моделирования специалист уже представляет конечный результат, его цель — только конкретизация количественного измерения результата.

9. В субъектно-объектной модели сделан по сравнению с другими моделями значительный шаг вперед, так как рассмотрены механизмы и методы создания ИПС (изолированной программной среды) как приоритетной задачи защиты информации. Действительно, в условия всех основных моделей входит некоторое безопасное начальное состояние, но в рамках моделей не рассматриваются конструктивные механизмы его достижения. СО-модель отвечает на этот вопрос, дополняя, а не отвергая другие модели. Формируется иерархия моделей, где выделяются этапы генерации ИПС, поддержка ИПС и разграничение доступа как с помощью мандатных, так и дискреционных механизмов.

При этом СО-модели присущ и ряд серьезных недостатков. Очень сильным представляется требование аксиомы 5 об обеспечении *внешними* по отношению АС средствами условий *неизменности* конфигурации

субъектов АС, активизируемых до старта процедур контроля целостности. Действительно, невыполнение требований не позволит создать изолированную программную среду (ИПС), а как их реализовать, и что вообще понимается под такими средствами, нуждается в уточнении.

Представляется крайне актуальной задача перехода от модели изолированной программной среды (ИПС) к построению и анализу модели доверенной вычислительной среды (ДВС), свойства которой удостоверяются и поддерживаются инструментальными средствами защиты информации в процессе работы АС.

Глава 2. **ВЕРБАЛЬНАЯ МОДЕЛЬ ЭЛЕКТРОННОГО ДОКУМЕНТА**

В главе 1 установлена необходимость исследования системных особенностей электронного документа, его отличий от традиционного. Возникает резонный вопрос: какая же глубинная причина лежит в основе невозможности применения традиционных представлений о документе в случае электронной форме его реализации? И аналоговый, и электронный документы содержат идентифицированную информацию, так что их содержательное описание одинаково. И тот, и другой — средство, используемое для обеспечения взаимодействия субъектов экономики. Оба являются документами, пусть даже изготовленными по разным технологиям. Так ведь и традиционный документ может быть рукописным, а может быть создан на основе последних технологических достижений, как, например, денежная купюра. Более того, на прежних этапах развития вычислительной техники, 20—30 лет назад, особых недоразумений, обусловленных спецификой технологии изготовления ЭлД, не возникало.

Единственное, что кардинально изменилось с тех пор, это среда функционирования документа. Раньше электронная форма документа была всего лишь технологическим эпизодом в его жизненном цикле, когда он именовался «документ на машинном носителе». На современном этапе для огромного количества документов, которые и понимаются как ЭлД, электронная форма становится постоянной в течение всего или почти всего жизненного цикла. Следовательно, электронная форма означает не столько количественное, сколько качественное усовершенствование технологии изготовления документа.

Документ может быть представлен либо в аналоговом, либо в электронном виде. Каждый из них имеет место только в присущей ему среде существования — аналоговой или электронной. Эти две среды не пересекаются, преобразование формы отображения документа может

иметь место только на границе сред и осуществляется на основе интерфейсных устройств преобразования аналоговых сигналов в электронные и обратно. В каждой среде действуют свои специфические законы, распространять действие которых за пределы среды некорректно [8, 12, 64].

2.1. Аналоговая и электронная среда существования документа

Сам по себе документ имеет место только в обществе мыслящих субъектов, так что и аналоговая, и электронная форма его существования, по сути, есть ни что иное, как некоторые технологии, основанные на присущих мыслящему субъекту способах восприятия и обработки информации. Для аналогового документа это очевидно непосредственно, для электронного документа — косвенно: законы и правила взаимодействия объектов электронной среды выбираются человеком с учетом физических законов, но исходя из законов мышления. В этом единство АнД и ЭлД: и тот и другой — документ, и тот и другой — отражает мышление и служит человеку.

2.1.1. Аналитическое и образное мышление

Общеизвестным является наличие у человека двух качественно отличающихся видов мышления: эмоционального (образного) и аналитического (абстрактного). В чистом виде каждый из видов встречается редко, с позиций диалектики образное и абстрактное мышление неразделимы. Тем не менее, в подавляющем большинстве ситуаций можно говорить о преобладании того или иного вида. С целью конкретизации системных характеристик среды, где эти виды доминируют, дальнейшие рассуждения намеренно «огрубляются», абсолютизируя выделяемые особенности.

Эмоциональный способ основан на образном восприятии: узнавании некоторого предмета, процесса, явления «в целом», отождествлении его с имеющимся «образом». Формирование образа основано на имеющемся «опыте, знаниях» человека. В контексте документа это реальный опыт, накопленный и обобщенный *обществом* в виде знания и переданный *человеку* в процессе его *обучения*. Обучение — процесс длительный, реализующий преобразование знания общества в опыт конкретного человека. Язык, письменность, понятийная база и т. д. — все это результат эволюции общества, переданный и закрепленный в индивидууме в процессе его обучения.

Цель обучения — выработка адекватной реакции субъекта на класс «похожих» объектов. Концепция обучения — последовательное предъявление субъекту серии аналогов, незначительно отличающихся объектов одного и того же класса, и закрепление (поощрением или наказанием) правильной реакции на образ. Появление предмета вызывает цепную реакцию неразделимых и потому кажущихся одновременными процессов: выявление характерных, реперных точек; отождествление их с закрепленными в процессе обучения в сознании; идентификация образа; трансформация образа в понятие. Образное восприятие — это принципиально *целостный, одномоментный* (die Gestalt, нем.) процесс.

Природа образного восприятия до конца не раскрыта. Здесь важно, что на «входе» человеку предъявляется некое бесконечное число точек, а «на выходе» формируется образ, идентифицируемый некоторой конечной совокупностью понятий. Человек «читает» не буквы, а слова, фразы. Он «видит» не «кусочек» картины, а всю или значительный фрагмент. «Слышит» не отдельную гармонику, а звук в целом.

Восприятие аналогового документа базируется на образном мышлении, интерпретации его содержания на основе знания, опыта, которым обладает субъект, взаимодействующий с документом. Здесь

понятие информации как знания, сведения уместно и содержательно, но понятие однозначности в аналоговой среде существования документа должно трактоваться достаточно широко: образное мышление принципиально базируется на «похожести», «приблизительности». Результат образного узнавания и восприятия в общем случае неоднозначен, приблизителен. Можно сказать лишь то, что предъявленный образ похож на образ, закрепленный в процессе обучения.

Аналитическое мышление абстрактно, основано на установлении причинно-следственных связей некоторых характеристик предмета, процесса, явления на основе совокупности абстрактных, логических правил типа «если выполнено $\alpha, \beta, \gamma, \ldots$, то выполняется $a, b, c, \ldots$ ». Для аналитического мышления характерна детерминированность, однозначность результата. Если однозначный результат не может быть получен, то это означает необходимость расширения исходной базы. В наиболее чистом виде абстрактное мышление характерно для математики.

Логика базируется на конечном числе исходных положений, вводимых аксиоматично, все остальные результаты по существу есть прямое следствие, *однозначно* вытекающее из принятой аксиоматической базы. В этом сила, но в этом и слабость логических заключений: для любого, пусть даже очень «неочевидного», сложного логического вывода достаточно крайне ограниченной исходной базы, но сам процесс установления справедливости заключения может состоять из огромного числа промежуточных этапов. Допущенная на любом из этапов ошибка приводит к неверному ответу. Аналитическое мышление, как базирующееся на логике, принципиально представляет собой последовательный процесс.

Коль скоро логическая обработка приводит к однозначному результату и базируется на конечном числе исходных положений (аксиом), то этот процесс, в принципе, может быть формализован. Формализация

означает возможность вывода заключения на основе алгоритма — набора *точных* инструкций (предложений), описывающих, как получить решение определенной задачи. Нетрудно придумать автомат, который действовал бы по некоторому алгоритму без вмешательства человека. А существует ли универсальный автомат, который можно было бы запрограммировать на выполнение *любого* алгоритма? Здесь мы входим в область *метаматематики*, объектом которой служит довольно ограниченный, казалось бы, набор правил, относящихся к математической логике, и которая занимается изучением самого процесса доказательства, логического вывода конечных предложений и утверждений на основе исходного набора постулируемых аксиом [65].

В своей знаменитой теореме Гёдель доказал, что любая система аксиом является неполной и не может быть сделана полной добавлением никакого конечного числа аксиом. Грубо говоря, в рамках любой формальной системы можно сформулировать предложение (формулу), которое не может быть ни доказано, ни опровергнуто в рамках этой системы. *Формальная система* состоит из конечного множества символов и конечного числа правил, по которым эти символы можно объединять в формулы или предложения. Некоторые из этих предложений являются исходными, и тогда они называются аксиомами. Повторное применение правил системы позволяет получить все новые и новые доказуемые предложения. Доказательство формулы представляет собой цепочку предложений, в которой каждое является либо аксиомой, либо выводится при помощи правил данной системы из предшествующих предложений.

Однако утверждение, что некоторая последовательность формул образует (или не образует) доказательство некоей формулы, уже не является предложением *в рамках* данной формальной системы, это предложение *о самой* системе. Такие предложения обычно называют метаматематическими.

Не вдаваясь далее в эту достаточно тонкую сферу, можно лишь отметить, сколь глубокая разница лежит между образной и аналитической обработкой информации. В частности, можно утверждать, что аналоговый и электронный документы есть объекты, вообще говоря, разных формальных систем. Отсюда следует, что их полная взаимозаменяемость в общем случае недостижима. Всегда, при любом уровне развития техники, будут существовать такие области применения документа, в которых возможно использование либо только аналогового, либо только электронного документа.

Английский математик Алан Тьюринг предложил очень простую *формальную систему*, которая, тем не менее, настолько богата, что способна воспроизводить чрезвычайно широкую гамму алгоритмов. Так называемая машина Тьюринга реализует предложенную им формальную систему. Его работа стала теоретической базой для создания современных ЭВМ. Зачастую даже определяют алгоритм как такую последовательность операций, которая может быть реализована машиной Тьюринга.

Так как инструкции алгоритма точны, то каждой из них можно поставить в соответствие некоторое число, и тогда реализация любого алгоритма сводится к операциям с числами. Естественным образом приходим к цифровой обработке информации. Электронное взаимодействие, базирующееся на точных логических правилах преобразования информационных сигналов, и понимается как среда цифровой обработки информации. Если выше, называя электронную среду цифровой, мы характеризовали технологическую реализацию, то сейчас выявлена фундаментальная основа такой эквивалентности.

Принципиальное различие логического и образного мышления объясняет невозможность адекватного описания электронного документа в категориях аналогового восприятия. Такое невозможно по определению: теория групп в математике имеет крайне далекое отношение к теории

групп в социологии, хотя некоторое подобие и можно уловить. В электронном документообороте должна существовать своя специфическая понятийная база. Тезис, что при электронном документообороте машина *самостоятельно* формирует и создает электронные документы, не должен вызывать неприятия. Если обработка документа и реакции на него есть строго формализованная последовательность операций, то это возможно. И это уже реализовано, например, в финансовых компьютерных системах. И как только в документооборот включается человек, то это означает выход из электронной среды в среду аналоговую.

Качественные отличия электронной и аналоговой среды так же масштабны, как отличия аналитического и образного мышления.

2.1.2. Понятие аналоговой и электронной среды

Конструктивное обсуждение свойств, характеристик, назначения документа не имеет смысла, если не исходить, хотя бы в достаточно общем виде, из свойств среды его существования. В рамках этой среды документ применяется, функционирует: создается, обрабатывается, хранится, передается, уничтожается. Говорить «вообще» о документе столь же бесплодно, как о скорости или длине тормозного пути автомобиля при строительстве гаража. Документ действенен только в рамках определенных технических, технологических, экономических, социально-политических ограничений, которые и характеризуют среду существования.

Говоря о традиционном документе, всегда по умолчанию неявно подразумевают аналоговую среду существования. Точно также, рассматривая электронный документ, надо исходить из законов электронной среды существования. «Очеловечивание» ЭлД, перенос понятий аналогового взаимодействия в электронную среду, ведет к абсурдным результатам. Качественное отличие аналогового и

электронного документов является следствием разных — в системном масштабе — характеристик аналоговой и электронной среды их существования. В связи с этим необходим анализ системных требований, предъявляемых к документу средой его существования.

Коренное отличие электронного и аналогового документов обусловлено их предназначенностью для функционирования в совершенно разных средах существования: *электронной* — среде программных и технических средств вычислительной техники; *аналоговой* — среде мыслящих субъектов, людей. К этим двум структурным составляющим информационного взаимодействия субъектов необходимо добавить третью — *интерфейс между аналоговой и электронной средой*. Так как деление документов на аналоговые и электронные обусловлено технологией, применяемой для отображения и движения содержащейся в них информации, то и среда существования документа должна характеризоваться технологией взаимодействия элементов среды с документом. Из общих соображений следует, что в таком случае должен выполняться принцип симметрии: каждой категории функциональных характеристик среды существования аналогового документа соответствует категория среды существования электронного документа. Наиболее общие соответствия очевидны: будь то АнД или ЭлД, имеют смысл понятия «создание», «формирование», «обработка», «передача», «хранение» документа.

В рамках среды существования можно говорить о «правах» и «обязанностях», которые документ налагает на элементы, образующие среду. Эти термины взяты в кавычки, так как «права» и «обязанности» характерны только для мира людей. Согласно теории интеллектуальных систем среда существования может быть образована и неодушевленными объектами. Тогда эти термины надо заменить, например, на «возможности» и «ограничения». При таком подходе документ,

объективная реальность, существующая вне нашего сознания, оказывается тесно связанным с внешними условиями, диктуемыми средой его существования.

Традиционный документ — это аналоговое отображение информации, закрепленное на твердом носителе и рассчитанное на непосредственное восприятие субъектом-человеком. Субъект обладает знаниями, способен к восприятию графического представления информации, ее «пониманию» и обработке посредством мышления. Базой восприятия является органически присущий человеку мощнейший аппарат распознавания образов, позволяющий ему отождествлять компоненты документа со сформированными в сознании эталонами. Традиционный документ имеет место только в общественной среде мыслящих субъектов — *аналоговой среде существования.* «Понимать» и адекватно реагировать на АнД может только мыслящий субъект.

Документ — явление социальное, его цель — формальное основание тех или иных действий субъектов, взаимодействующих при его помощи. Поэтому трактовка документа субъектами не может быть произвольной, иначе ни о каком взаимодействии, предполагающем взаимную обусловленность их поведения, не может быть и речи. Следовательно, существует некоторая внешняя сила, задающая законы формирования и восприятия человеком аналогового документа. Текст документа должен удовлетворять многочисленным правилам языка и письменности, стиль изложения должен соответствовать неформальным этическим ограничениям профессиональной среды, оформление должно быть выполнено на основе действующих стандартов. Даже объем и содержание документа ограничено достаточно жесткими рамками его функционального назначения. В роли диктатора выступает как формальный представитель общества — государство, так и неформальный — сложившийся менталитет, обычаи и правила общественного поведения.

Распространенное мнение, что человек формирует и обрабатывает традиционный документ самостоятельно, произвольно, при более тщательном рассмотрении оказывается неверным. Создатель документа далеко несвободен в своих действиях и должен подчиняться весьма жестким правилам и ограничениям. Произвол возможен в весьма узком диапазоне, несопоставимом по масштабам с теми правилами, которые обязаны выполняться в аналоговом документе. Ограничения кажутся настолько естественными и «само собой разумеющимися», что их влияние зачастую не замечается, так же, как необходимость уметь говорить, писать.

При создании, обработке и хранении аналогового документа общество, профессиональная среда непосредственно или через своих представителей (государство, организация, социальная группа, семья) выступают относительно субъектов информационного взаимодействия в качестве некоей «внешней силы». Соблюдение диктуемых этой силой формальных и неформальных приказов и распоряжений поощряется, а их нарушение наказывается. Человек всего лишь интеллектуальный исполнитель, действующий в рамках довольно жестких общественных предписаний. Общество, социальную группу, *нельзя* отождествлять с каким-либо отдельным человеком, это качественно иное образование.

Аналоговая среда существования документа — система субъектов (людей), структурно объединенных в единое целое и взаимодействующих на основе диктуемых обществом неформальных (язык, традиции, обычаи и пр.) и формальных (нормативная правовая база) правил обработки, хранения и передачи информации, представленной в образной форме. Правила вырабатываются обществом — внешней относительно любого субъекта силой, и базируются на причинно-следственных взаимосвязях различных явлений (образов), сформировавшихся в процессе развития и становления общества.

Среда существования ЭлД должна образовываться элементами, способными реагировать на него, эту среду мы называем электронной. Есть ли в этой среде место человеку, может ли человек воспринимать электронный документ? На первый взгляд, очевиден утвердительный ответ, аргументируемый «неоспоримым» доводом, что предназначенное для человека изображение документа на экране монитора или его распечатка на принтере и есть электронный документ. Однако если тщательно проанализировать этот довод, то его «неоспоримость» не кажется столь очевидной.

Распечатка — документ на бумажном носителе, следовательно, это аналоговый документ. Изображение документа на экране монитора ничем принципиально не отличается от проекции аналогового документа — диапозитива — на киноэкран или от воспроизведения голограммы. Происходит неявная подмена объекта: вместо *исходного*, электронного документа, мы говорим о *производном* документе, аналоговом. Это два разных, хотя и функционально связанных, документа. Печатание на принтере или изображение на мониторе по существу представляет собой реализацию конкретного способа изготовления аналогового документа, наравне с рукописным, машинописным, типографским. Способ восприятия и способ изготовления далеко не одно и то же: аналоговый документ предназначен для человека, электронный — для компьютера.

Экран монитора — это граница (интерфейс) между электронной и аналоговой средой существования: «снаружи» монитора аналоговая среда, «внутри» — электронная. «Снаружи» документ рассчитан на восприятие субъектом среды, человеком, значит, это документ в аналоговой форме. «Внутри» монитора документ предназначен для обработки неодушевленными объектами электронной среды, он представлен в виде последовательности (множества) сигналов, импульсов. Эта последовательность не может непосредственно восприниматься

человеком, она предназначена для воздействия на объекты совершенно иной физической природы, являющиеся элементами *электронной* среды существования документа.

Человек вынужден ограничиваться восприятием иного, аналогового документа, имеющего некоторое отношение к исходному ЭлД. Количественно это может быть достаточно далекое отношение: например, страница текста — это порядка 1500 байт информации, тогда как в памяти ЭВМ она занимает в несколько раз больший объем при графическом формате представления, или — меньший, при использовании архивирования. Отождествлять ЭлД и «картинку» это примерно то же самое, что приравнять звук из динамика модулированному несущему радиосигналу.

Кардинальное отличие физической среды существования документа ведет к принципиальному отличию электронного и аналогового документов. Электронный документ есть цифровое отображение информации, носителем которого являются средства вычислительной техники и информатики. ЭлД непосредственно воспринимается только объектом электронной цифровой среды — техническим или программным средством. Только объект электронной среды может обрабатывать электронный документ: выполнять априорно заданное детерминированное преобразование входного ЭлД в выходной ЭлД. Электронный документ имеет место только в электронной (цифровой) среде существования.

Но из этого следует, что человек «исключается» из электронного взаимодействия, и электронный документ «создает» (формирует) не человек, а машина. Некорректное определение содержания терминов «исключается», «создает (формирует)» приводит к неявному переносу сложившихся в аналоговой среде понятий за область их значимости. При создании аналогового документа человек весьма ограничен в своих действиях, правила и ограничения задаются внешней по отношению к

субъекту силой — обществом, которое можно считать «руководителем». Так, принято говорить, что законы не имеют авторов, они создаются и принимаются обществом.

Тем не менее, считается, что АнД создается конкретным человеком, но не обществом. А вот по отношению к электронному документу «правила игры» меняются, хотя несомненным является требование постоянства логических позиций анализа, их независимости от технологии формирования и обработки документа. В электронном документообороте человек выполняет такую же роль, что и общество — в традиционном. Человек, распоряжающийся электронной средой существования ЭлД, является «внешней силой», «высшей инстанцией», «диктатором» по отношению к элементам среды, он устанавливает «правила игры»: выбирает стандарты технологического взаимодействия, архитектуру среды, выбирает сами элементы — технические и программные средства. «Машина может все, задача человека — ограничить ее, заставить делать только то, что нужно» — писала когда-то по поводу выпуска ЭВМ «Наири» Мариетта Шагинян. То же самое делает и общество по отношению к человеку в аналоговой среде.

Говоря о традиционном документе, люди остаются в рамках среды существования АнД, обходятся без упоминания общества, сводят задачу к взаимодействию его элементов, субъектов, посредством документа. И такой подход оправдан многовековой практикой традиционного информационного взаимодействия. Однако, как только дело касается электронного документа, вводится внешний объект относительно среды существования электронного документа — человек. Хотя уже сейчас имеется огромное количество ситуаций, когда компьютер самостоятельно, без какого-либо вмешательства человека, создает новые электронные документы.

Платформа анализа должна быть единой: если в аналоговой среде рассматриваются только прямые участники информационного взаимодействия, то и в электронной надо поступать также.

Теперь можно опровергнуть наиболее частый аргумент в пользу непосредственного взаимодействия человека с ЭлД: «именно человек создает электронный документ, нажимая на буквы-клавиши клавиатуры; каждая отдельная буква есть, пусть очень короткий, но все-таки аналоговый документ, значит, аналоговый документ существует в электронной среде». На самом деле, в электронную среду вводится не аналог, а совокупность из нескольких двоичных сигналов, это, пусть и «очень короткий», но электронный документ: машина воспринимает не АнД-букву, но ЭлД-знак. Чтобы убедиться в этом, достаточно, например, перейти от русского алфавита к английскому: клавиша (буква) та же самая, но образ иной (для сравнения, слово «документ» при наборе на латинице будет введен как «ljrevtyn»). Значит, это не человек, но компьютер «решил», что вводить.

При создании электронного документа на машине реализуется априорно заложенная в компьютер программа формирования итогового электронного документа из других, инициированных воздействием человека на клавиатуру, *уже находящихся* в ЭВМ «маленьких ЭлД» — байтов символов, соответствующих буквам. Инициировать ЭлД, запустить процесс, нажать на клавишу, «повернуть рубильник» — далеко не одно и то же, что создать документ, реализовать процесс. Для запуска не требуется восприятия человеком электронного документа.

Воспринимать цифровую последовательность может только компьютер, и не может человек. Среда существования электронного документа образована объектами цифровых технологий. Но здесь реакция на документ объектов среды, программных и технических средств вычислительной техники, диктуется не обществом, как в случае с АнД, а

непосредственно владельцем и/или пользователем компьютера: выбранными архитектурой, стандартами, параметрами технических и программных объектов. Создается свой, цифровой (электронный) мир существования документа.

Электронная (цифровая) среда существования — система объектов (технических и программных средств вычислительной техники), взаимодействующих на основе формальных правил (архитектура, стандарты, технические параметры устройств, языки программирования и пр.) обработки, хранения и передачи информации, представленной в цифровой форме. Правила устанавливаются внешней силой относительно любого элемента среды — человеком, и базируются на объективных физических и логических законах.

Качественная несопоставимость образного и логического восприятия и обработки информации отражается в радикальных различиях математических моделей, описывающих аналоговый и электронный документы. Если документ интерпретировать в виде множества, то задача сопоставления аналогового и электронного документов сводится к изучению свойств соответствующих множеств. Ограничимся понятийным уровнем, заведомо огрубляя строгие математические термины. Так как нас интересуют процессы восприятия и обработки документа субъектом аналоговой или объектом электронной среды, то, прежде всего, надо уточнить, что же именно *воспринимается* и что именно *обрабатывается*. Понятия аналоговой и электронной среды, образного и аналитического восприятия создают необходимые стартовые предпосылки для анализа.

2.1.3. Модель аналогового документа в виде предмета-множества и его свойства: бесконечность, непрерывность, статичность (фиксированность). Целостность АнД

Исходным для формирования образа аналогового документа является предъявление субъекту некоторого предмета (лист бумаги с текстом), образованного совокупностью (множеством) элементов. Множество, моделирующее аналоговый документ, организовано по закону очередности: положение любого элемента относительно остальных удовлетворяет определенным ограничениям, не жестким (лист можно свернуть, согнуть и т. д.), но и не произвольным (лист нельзя разорвать). Элементы множества могут принадлежать разным классам: отличаться по цвету, структуре, плотности и т. д. Не обязательно двумерное размещение элементов, достаточно вспомнить вклеенную в «толщину» денежной банкноты полоску с указанием номинала. Отсутствие такой полоски свидетельствует о поддельности банкноты, т. е. лишает ее статуса документа.

Важно, что образ документа создается *всем* множеством элементов различных типов, в том числе и носителем информации, а не каким-либо подмножеством. Другое дело, что требования к образу аналогового документа не имеют четких границ, не носят пороговый характер. Оторванный уголок листа или пропущенная буква в тексте не меняют идентификацию объекта как документа. Но если отрывать все большую и большую часть, то наступает момент, когда предъявляемый лист с текстом уже не будет идентифицироваться субъектом среды как документ. Элементом больше или меньше, не всегда имеет значение, именно потому, что *образ аналогового документа создается множеством с чрезвычайно большим количеством элементов*. Теоретически можно полагать, что множество как математическая модель аналогового документа содержит *бесконечное* количество элементов (имеет бесконечную мощность).

На первом этапе восприятия аналогового документа содержащаяся в нем информация не играет никакой роли. Оформленное в соответствии с устоявшимися стандартами письмо фирмы на японском языке будет

восприниматься как документ, хотя для субъекта совокупность иероглифов не является сведением, знанием, информацией (согласно определениям аналоговой среды). Значение имеет лишь соответствие сложившимся у человека представлениям о стандартном облике служебных документов, создаваемом носителем и расположением темных и светлых элементов его поверхности.

Любой документ может содержать только конечный объем информации, понимаемой как сведения, знания. Это же вытекает из конечности различных информационных символов (знаков), содержащихся в тексте документа. В принципе для отображения информации документа достаточно конечного подмножества элементов из того бесконечного множества элементов, которые образуют сам документ. И это было бы достижимо, если каждой идентификации информационного символа (буквы, знака) соответствовало бы *одно и только одно* его изображение.

В аналоговой среде подобное невозможно в силу принципиальной неисчерпаемости среды и приблизительности образного восприятия. Здесь одной и той же идентификации соответствует бесконечное число вариантов изображений символа. Но бесконечное число модификаций может быть получено, только если образ знака образуется бесконечным числом элементов. Даже точка в аналоговом изображении — это совокупность очень близко расположенных точек меньшего размера, сливающихся, при взгляде со стороны, в более крупную. Таким образом, *информация аналогового документа отображается подмножеством бесконечной мощности*.

Согласно модели на «вход» субъекта одномоментно поступает бесконечное множество элементов, воспринимаемое им как образ документа. Далее субъект выделяет из этого множества подмножество, опять-таки бесконечное, которое воспринимает как образ информации.

Переработка бесконечного множества точек образа приводит к конечной совокупности идентификаторов: букв, слов, фраз: формируется восприятие сообщения [81]. И только затем, в результате обработки конечного множества, человек приходит к трактовке информации как сведения, знания. В аналоговой среде всегда должен существовать особый этап, качественно отличный от всех других, этап перехода количества в качество, этап перехода от *бесконечного к конечному*.

Так как за конечное время можно обработать только конечное число сигналов, то входное бесконечное множество должно быть организовано таким образом, чтобы его можно было описать на основе выборки конечного числа элементов. Это свойство обозначим как *непрерывность* множества, отображающего информационные знаки в аналоговом документе (непрерывная функция, содержащая бесконечное число точек, с любой наперед заданной точностью может быть описана конечным числом промежуточных значений). Здесь используется понятийная трактовка, хотя с позиций математики это не совсем корректно: термины, характеризующие структуру множества (мощность, непрерывность, плотность, компактность, сепарабельность и пр.), достаточно специфичны и строго определены.

На практике непрерывность не кажется столь очевидной и обусловленной. Например, если текст документа напечатан игольчатым принтером, то на человека как бы воздействует конечное дискретное множество точек. Но нельзя забывать, что при распознавании знака сопоставляется расстояние между соседними точками с расстоянием между соседними знаками, а расстояние, длина, есть не что иное, как мера на множестве, в данном случае представляющем собой бесконечное число точек листа, на котором напечатан текст.

Если расстояние между точками настолько велико, что взгляд охватывает только две соседние точки, формирующие букву, то, двигаясь

по часовой стрелке от левой нижней точки буквы Н, ее легко принять за букву П. Чтобы распознать букву, необходимо видеть все пространство, т. е. бесконечное множество точек. Разбросав «соседние» буквы по определенному закону по поверхности листа, можно ликвидировать непрерывность. Именно так делается при использовании шифров замены, когда «соседние» точки исходного изображения перемещаются в разные области. В этом случае, например, изображение черно-белых клеток шахматной доски сводится к некоторому серому фону [66. С. 129]. А ведь вся информация сохранилась неизменной, и клетки доски могут быть однозначно восстановлены в силу обратимости алгоритма.

Субъект аналоговой среды обладает способностью к выделению из воспринимаемого им бесконечного непрерывного множества конечного подмножества реперных точек, которые и обрабатывает в дальнейшем: создает образ буквы, ассоциирует в слово конечное число букв, отождествляет слово с его значением, объединяет значения конечного числа слов в виде сведения. Вся обработка ведется над конечными множествами, что принципиально возможно, но для этого этап перехода от бесконечности к конечности, от непрерывности к дискретности в аналоговой среде обязателен. Реперные точки не заданы заранее, каждый раз, когда мы смотрим на изображение символа, мы выделяем разные подмножества, хотя, как правило, близкие. Это не влияет на результат в силу непрерывности входного множества-знака, но это означает, что сама проблема выбора реперных точек требует *одномоментного* воздействия всех элементов входного множества.

Нельзя за конечное время скопировать бесконечное число элементов, значит, не могут быть изготовлены два тождественных аналоговых документа. Любые два АнД обязательно чем-то отличаются, каждый из них имеет индивидуальные особенности, их можно сопоставить, они *различимы*. В таком случае различимость можно использовать как ресурс

для классификации. В зависимости от степени различий множеств, представляющих два документа, можно выделить «идентичные» документы, *различные* «экземпляры» АнД, «подлинник» и «копию», и т. д.

Для того чтобы бесконечное множество элементов можно было бы воспринять за конечное время, необходимо *одномоментное* предъявление субъекту этого множества или, по крайней мере, его значительной части. Но это означает существование в данный момент всего множества (или фрагмента) целиком, т. е. свойство *фиксированности* принципиально присуще аналоговому документу.

Так как в бесконечном количестве элементов аналогового документа как множества собственно информация (не образ, а смысл) эквивалентна конечному подмножеству, то налицо огромная избыточность аналогового документа. А любая избыточность есть ресурс для решения прикладных задач, в том числе, для обеспечения защиты аналогового документа. Яркий пример — защита подлинности денежной купюры.

Вот в какой тесный узел оказываются завязанными свойства бесконечной мощности, непрерывности и фиксированности множества — математической модели аналогового документа — и свойство целостного восприятия этого множества субъектом аналоговой среды. Любое из свойств обусловлено остальными и потому не может быть исключено. В реальном мире бесконечность, непрерывность, целостность не осознаются, это математическая идеализация, своего рода предельный случай и как любой предельный случай, позволяет выделить и объяснить характерные особенности объекта, процесса, явления.

2.1.4. Модель электронного документа в виде процесса-множества и его свойства: конечность, дискретность, динамичность

Все информационные технологии, реализуемые на основе средств вычислительной техники и информатики, базируются на использовании законов логики. Логический вывод – это *последовательная* цепочка детерминированных заключений, и ни одно из заключений нельзя сделать, если не выполнены предыдущие заключения. Детерминированность означает однозначность заключения, если, конечно, оно может быть получено: часто случается, что исходных положений недостаточно, и тогда заключение отсутствует. Если в машину не ввести положение о невозможности деления числа на нуль, то ЭВМ неизбежно прекращает работу, сигнализируя об аварийной остановке. Для «запуска» логического процесса вывода необходимо *точное* задание начальных условий, исходной информации.

Процесс логической обработки *необходимо должен иметь последовательный характер*. Этот процесс необходимо должен быть *дискретным*, поэтапным, должна существовать четкая граница конца и начала каждого этапа. Число таких этапов может быть очень велико, но обязательно *конечно*, иначе время обработки равнялось бы бесконечности. Любой этап логической обработки характеризуется *конечным* числом обрабатываемых входных сигналов. Это вытекает как из самих логических постулатов, так и из последовательного характера формирования вывода. Следовательно, при электронном взаимодействии документ может отображаться только в виде множества *конечной* мощности.

Машина Тьюринга иллюстрирует, в некотором смысле, предельный случай реализации логической обработки: на каждом шаге операции производятся всего с двумя знаками. Какие бы усовершенствования ни были бы в будущем сделаны в классе тьюринговых машин, нельзя уйти от требования *конечности* множества обрабатываемых сигналов, его дискретности, *последовательного характера* выполнения *дискретных* операций и *последовательного характера* ввода информации. Как и выше,

рассмотрим качественные следствия, которые вытекают из предлагаемой модели документа в электронной среде.

В силу конечности множества и конечности категорий элементов, его образующих, в принципе, всегда можно создать абсолютно тождественную «копию» (в традиционной терминологии) «оригинала» электронного документа. Эта «копия» ничем, в смысле восприятия и логической обработки, не будет отличаться от «оригинала», их даже теоретически невозможно отличить друг от друга, они *неразличимы*. Следовательно, нельзя применительно к электронному документу говорить об экземплярах ЭлД, идентичных ЭлД, подлиннике и копии ЭлД и т. п. Либо это один и тот же электронный документ, либо — два разных документа. Подробнее это положение будет рассмотрено в разделе, посвященном понятию электронной информации.

Специального анализа требует понятие фиксированности электронного документа. С одной стороны, само *существование* документа автоматически предполагает его целостность в любой момент времени его жизненного цикла, т. е. *фиксацию* в той или иной технологической форме. С другой стороны, дискретность множества, последовательный характер логических операций с его элементами, обработка машиной Тьюринга в каждый момент времени всего двух элементов *исключает фиксацию*. В идеологическом плане любая ЭВМ есть та же самая машина Тьюринга, так что противоречие сохраняется.

Парадокс устраняется, если допустить *две формы существования электронного документа: статическую и динамическую*. В статической форме документ находится во время хранения в памяти. Статическая форма характерна для аналоговой среды. Здесь электронный документ можно рассматривать как аналоговый объект. Например, давно вышедшая из употребления перфокарта фактически есть аналоговый документ, только с весьма специфическим «алфавитом». Это утверждение сомнения

не вызывает. Но ведь диск памяти функционально та же самая перфокарта, только роль отверстий играет ориентация магнитных доменов.

Электронный документ реально используется для решения прикладных задач только в активизированном (динамическом) состоянии. Пассивное (статическое) состояние ЭлД (в памяти компьютера) – это лишь вспомогательный этап, необходимая предпосылка активизации. Говорить о фиксации динамического состояния бессмысленно, так как в каждый момент времени наблюдается только очень малая часть документа. Для индикации всего документа принципиально необходим конечный временной интервал. Абсолютизация фиксированности ЭлД не является необходимым условием его существования, более того, исключает активизацию документа, в том числе, получение на основе ЭлД аналогового документа. Например, на экране монитора изображение развертывается со скоростью более миллиона пикселей в секунду. Да и в пассивном состоянии свойство фиксированности ЭлД неконструктивно: где-то в памяти, но где именно, неизвестно. К тому же и сама физическая реализация записи фрагментарна: часть в одном месте дискеты или диска памяти, часть — в другом.

Активизированный электронный документ — это динамический процесс последовательных преобразований некоторого множества сигналов.

Конечность множества, отображающего электронный документ в целом, означает, что избыточность электронного отображения информации много ниже, чем в случае аналогового документа. Но избыточность и есть тот ресурс, который можно использовать для обеспечения вспомогательных функций документа! Этот ресурс позволяет добиться обеспечения помехоустойчивости, защищенности, юридической значимости документа и др. Как следствие, проблемы защиты, обеспечения правомочности документов в электронной среде реализуются

принципиально много сложнее, чем в среде аналоговой. «Бесплатно» ничего сделать нельзя, чем меньше ресурс — тем (при прочих равных) хуже результаты.

Программные средства (ПС) как объекты электронной среды вполне могут рассматриваться как тот же электронный документ, пусть своеобразный: обычный документ содержит информацию о «факте», программа содержит информацию о «процессе». Как и ЭлД, программа включает «содержание» и «атрибуты». Последние являются ресурсом для защиты ПС, т. е. для защиты конкретного процесса преобразования и обработки ЭлД. Кардинальное увеличение такого ресурса можно обеспечить только переходом к аналоговым атрибутам ПС. Но это означает аппаратную реализацию преобразования в виде некоторого модуля, тогда защита реализуемого программой процесса от несанкционированного доступа (НСД) обеспечивается за счет аналоговых атрибутов модуля. Таким образом, *применение аппаратных средств защиты ЭлД от НСД принципиально имеет очень высокий потенциал*.

2.1.5. Содержание и атрибуты документа. «Приблизительность» аналоговой среды и «точность» электронной среды

Любой документ состоит из двух компонентов: один из них — *содержание* — реализует прямое, информационное назначение документа; другой, который будем называть *атрибутами*, реализует вспомогательные функции — обеспечивает необходимые условия для восприятия и обработки документа и придает содержащейся информации статус документированной.

По своему назначению атрибуты можно разделить на два класса: справочные и сервисные. Справочные атрибуты отражают служебную информацию, например, адрес, телефон, регистрационные данные и др. Таковыми являются большинство параметров, обычно называемых

реквизитами документа. Служебная информация должна быть неизменной во времени и в пространстве, поэтому справочные атрибуты можно присоединить к содержанию и рассматривать как его часть. Сервисные атрибуты (аналогового или электронного) документа понимаются как совокупность качеств (параметров) документа, обеспечивающих возможность прикладного применения выбранной технологии информационного взаимодействия. Далее именно сервисные атрибуты понимаются под термином «атрибуты».

Фигурально выражаясь, атрибуты — это некоторая оболочка для содержания документа, это та «упаковка», «коробочка», в которую заключено содержание. Как и всякая упаковка, атрибуты документа выполняют вспомогательные функции, в данном случае — справочные, юридические, технологические. В том числе потребительские функции удобства применения *данного* документа (доступность), сохранения его целостности, обеспечения конфиденциальности, аутентификации субъектов (объектов), взаимодействующих с *данным* документом. Таким образом, атрибуты, вернее их совокупность, должны быть достаточно прочно связаны (в идеале — неотделимы) с содержанием именно этого, конкретного документа.

Возможны два типа реализации подобной взаимосвязи: на физическом и логическом уровнях. Первый тип базируется на свойствах физической реализации документа, физические параметры документа должны соответствовать определенным требованиям, точнее, параметрам соответствующего эталона. Второй тип основан на вычислении однозначно определенной функциональной зависимости от содержания документа и, опять-таки, последующем сопоставлении результата с заданным или вычисляемым эталоном.

В аналоговой среде в подавляющем числе случаев используются физические атрибуты. Для создания образа документ реализуется в виде

предмета (текст на листе бумаги), раскраска, форма, структура которого позволяют субъекту, обладающему соответствующими знаниями, выделить содержащуюся в нем информацию, в том числе, и служебную. Любые два экземпляра АнД имеют различающиеся физические атрибуты, принимающие в силу непрерывности бесконечное число значений, пусть и в ограниченном диапазоне. Поэтому атрибуты отображаются в модели аналогового документа подмножеством бесконечной мощности. Любые физические характеристики предмета в аналоговом макромире не могут быть измерены абсолютно точно, поэтому эталон задает только допустимые границы, в которых должны находиться параметры. Именно атрибуты обусловливают «приблизительность» восприятия и обработки АнД.

Принципиально важно, что содержание аналогового документа, понимаемое не как «смысл», «знание», а как совокупность конкретных информационных символов, задается однозначно. Содержание документа не может меняться в зависимости от места в пространстве и времени. Приблизительность, неоднозначность обусловлена *восприятием* символов аналогового документа субъектом среды, не содержанием, но атрибутами документа. Важной функцией атрибутов аналогового документа является создание условий для обеспечения единственности интерпретации содержания документа.

Приблизительность есть неотъемлемое свойство аналоговой среды, характеризующее не только объекты среды, но и процессы в среде, не только восприятие документа, но и сам документ, не только в пространстве, но и *во времени*. Множество так называемых «идентичных» аналоговых документов, рассматриваемых в данный момент времени, например, тираж официальной публикации, есть совокупность, хотя и очень «похожих», но отличающихся один от другого экземпляров. Каждый из них — тот же документ, и каждый имеет одинаковую юридическую

силу. Эволюцию аналогового документа во времени можно также интерпретировать как множество документов, каждый из которых соответствует состоянию данного АнД в соответствующий момент времени. Элементы множества очень «похожи», но, разумеется, различаются. Документ стареет — желтеет бумага, выцветает печать, ветшают края. Тем не менее, это один и тот же аналоговый документ.

В аналоговой среде нет места «идентичности», здесь существует только «похожесть». Восприятие и/или обработка аналогового документа принципиально является приближенной, неоднозначной как в пространстве, так и во времени.

Лежащий в основе электронной среды логический тип восприятия и обработки информации удобен для задания и вычисления функциональных зависимостей. Физические атрибуты полностью не исключаются: например, точно так же, как лист бумаги содержит АнД, дискета содержит ЭлД. В статическом состоянии ЭлД может иметь физические атрибуты, но в активном состоянии его атрибуты всегда логические.

Электронная информация есть цифровое отображение сообщения, мы имеем дело с числом, а не с образом, как при аналоговом отображении. Число — это точность, тогда как образ — это нечеткость, приблизительность, похожесть. В этом смысле цифровая, электронная среда отличается от аналоговой среды кардинально. Ошибки восприятия и обработки электронного документа обусловлены «шумом», а не принципиальными особенностями среды. Если ЭлД «не читается» сейчас, то и все последующие попытки с таким же набором операций будут безуспешны. Результат обработки одного и того же ЭлД на разных ЭВМ всегда будет один и тот же, если среды обработки аналогичны.

Поскольку информация, содержащаяся в документе, отображается конечным подмножеством элементов, а логический атрибут есть функция от информации, то атрибуты ЭлД также отображаются конечным

подмножеством. Что вполне согласуются с конечностью множества, отображающего электронный документ в целом. Из постоянства информации ЭлД сразу вытекает постоянство его логических атрибутов. При логической обработке цифровой последовательности нет места случайности. Даже программа генерации «случайных» чисел выдает на самом деле строго детерминированную последовательность. Каждое следующее число однозначно определяется алгоритмом и предыдущими числами, т. е. оно неслучайно: зная исходные установки, всегда можно вычислить любой элемент последовательности. Чтобы реализовать случайность, принципиально необходимо выйти за рамки электронной среды в аналоговую – например, использовать физический источник «шума».

В электронной среде нет места «похожести», здесь существует только «идентичность». Восприятие и/или обработка электронного документа принципиально является точной, однозначной как в пространстве, так и во времени.

В таком случае и результат сопоставления двух электронных документов должен быть однозначен: либо это «точно то же самое» — если выполняются критерии сравнения; либо «совершенно разное» — если не выполняются. Теряет смысл само понятие «экземпляр» электронного документа: не может быть «другим» (экземпляром) «точно то же самое». Понятие «то же самое» достаточно тонкое, в математике принято говорить о *неразличимых* объектах.

Поэтому электронный документ нужно интерпретировать как ***множество*** *неразличимых (одинаковых) реализаций*. Находит системное объяснение рассмотренная ошибка законов о множестве оригиналов (экземпляров) электронного документа. *Все* множество реализаций есть *единственный* оригинал электронного документа. Свойства множества, т. е. свойства оригинала ЭлД, определяются по любой реализации, ведь все

остальные «точно такие же». И если ЭлД должен использоваться однократно (платежное поручение), то однократной должна быть идентификация множества, но не реализаций.

Дисциплина идентификации, например, электронного платежного поручения, может быть выбрана произвольно: по первой реализации; по двум из трех (мажоритарная логика); по неопределенному числу, если совокупность реализаций выводится на экран монитора, и др. Парадокса нескольких подлинников не возникает, меняется магистральное направление в технологической реализации электронного взаимодействия: *не обеспечение единственности реализации ЭлД, но гарантирование однократности регистрации* ***множества*** *реализаций*.

2.2. «Информация» в электронной среде

Установленные результаты делают очевидным невозможность дальнейшего базирования на подобии электронного и традиционного документов при решении специфических проблем электронного взаимодействия. Необходима существенная коррекция системных понятий электронного документа и, далее, электронного документооборота. Точность, присущая цифровой среде и цифровым операциям, предъявляет соответствующие требования к трактовке системных понятий электронного документа, влечет математизацию терминологии.

Различные определения понятия «информация» федеральных законов и законопроектов ориентированы на аналоговую среду существования документа, образованную мыслящими субъектами, людьми. Говоря об электронном взаимодействии, об электронном документе, необходимо исходить из требования эффективности терминологии применительно к описанию электронной среды,

формируемой неодушевленными объектами: программными и техническими средствами вычислительной техники и информатики.

В электронной среде нет ни знания, ни сведений: объектам среды, программно-техническим средствам ВТ это неведомо. Здесь понятие информации должно опираться на свойства информационного сигнала, а не на семантические характеристики. Машина не умеет мыслить, она умеет только преобразовывать выделенное тем или иным способом множество сигналов на основе *однозначно* заданных логических операций. В неживой природе объекты взаимодействуют с множеством сигналов, но не со «знанием» и «сведениями».

Электронная среда характеризуется обработкой и преобразованием информации на основе логических правил. Любой логический вывод — это совокупность *последовательно* выполняемых логических операций, поэтому множество, отображающее информацию, необходимо должно быть *последовательностью*. Это должна быть *конечная* последовательность, в противном случае число этапов ее обработки равнялось бы бесконечности, что нереализуемо физически.

Не всякое множество есть последовательность, а только то, на котором *задано* отношение порядка: правило, позволяющее для любой пары элементов множества установить предшествование одного другому. Заданное отношение порядка может отличаться от естественного. Множество чисел {7, 5, 7} можно считать последовательностью, если задать отношение порядка, например, слева направо. Тогда для пары чисел (7, 5) можно утверждать, что число 7 во множестве стоит левее числа 5, для пары (5, 7) — число 5 левее числа 7, а для пары (7,7) — одно из них стоит левее другого.

В таком случае говорят, что на множестве задано *бинарное отношение частичной упорядоченности*. Термин «частичной» обусловлен здесь допущением одинаковых элементов во множестве. Не всякий

признак может задавать отношения порядка. Например, для множества точек окружности нельзя выбрать признак «точка a предшествует точке b, если из a в b можно перейти по ходу часовой стрелки». Должны выполняться определенные ограничения. Признак частичной упорядоченности не может быть произвольным, необходимо выполнение определенных, хотя и довольно слабых, аксиом [67].

Пусть из множества X выбирается с возвращением пара элементов x_i, x_j (сначала один элемент x_i, который возвращается в множество, а затем другой элемент x_j; в частном случае может быть, что это один и тот же элемент, т. е. $x_i = x_j$). Если между элементами любой выбранной таким образом (и в таком порядке) пары устанавливается определенный тип соответствия, то говорят, что на множестве определено *бинарное отношение* φ. Тогда используется запись $x_i \varphi x_j$, причем порядок элементов существенен.

Бинарное отношение φ (используется также обозначение ≤) есть отношение частичной упорядоченности на множестве $X = \{x, y, z, ...\}$, если оно удовлетворяет следующим аксиомам:

- рефлексивности — $x\varphi x$, или $x \le x$;
- транзитивности — если $x\varphi y$ и $y\varphi z$, то $x\varphi z$, или — если $x \le y$ и $y \le z$, то $x \le z$;
- антисимметричности — если $x\varphi y$ и $y\varphi x$, то $x = y$, или — если $x \le y$ и $y \le x$, то $x = y$.

Всякая последовательность представима в виде множества пар элементов, в каждой из которых один элемент (например, левый) предшествует другому. Верно и обратное: если известно все множество пар элементов с заданным отношением предшествования, то исходная последовательность восстанавливается однозначно (для множества пар {(7,7), (7,5), (5,7)} исходное частично упорядоченное множество можно представить только в виде последовательности {7, 5, 7}). Таким образом,

можно обработать «сразу» всю исходную последовательность, а можно сначала обработать в *произвольном* порядке каждую упорядоченную пару ее элементов, и после этого восстановить исходную последовательность. Ситуация не меняется, если вместо упорядоченной пары элементов выбирать в *произвольном* порядке фрагменты последовательности, сохраняя заданное на фрагментах отношение предшествования.

Отношение упорядоченности отвечает принципам реализации машины Тьюринга — концептуальной основы современных вычислительных средств. Любое упорядоченное множество с точностью до изоморфизма восстанавливается на основе произвольного перебора всех возможных пар элементов с заданным для каждой пары бинарным отношением. Параллельная обработка множества («сразу!») сводится при этом к последовательной обработке ее фрагментов, именно так и производится преобразование «информации» в электронной среде. При этом *гарантируется* восстановление исходной очередности элементов множества по конечному результату преобразования, причем «смысл» информации, закодированной в виде последовательности, не имеет ни малейшего значения для обработки, существенен только порядок. Поскольку каждый раз рассматривается только два элемента, то обеспечивается применение логических действий, возможное только при конечном числе аргументов.

Основным требованием к документу как к агенту информационного взаимодействия является неизменность содержащейся в нем информации в пространстве и во времени. Именно поэтому в определениях аналогового документа делается акцент на его фиксированности. Согласно ГОСТ Р 51141–98 **[**30**],** закону «Об обязательном экземпляре документов» [24] — документ есть материальный объект с *зафиксированной* на нем информацией. Электронный документ реально используется для решения прикладных задач только в активизированном состоянии, пассивное

состояние ЭлД (в памяти компьютера) есть лишь вспомогательный этап, необходимая предпосылка активизации. Но именно активизированный ЭлД, как установлено выше, принципиально *не фиксируется*, это *процесс* последовательных преобразований некоторого множества сигналов. В электронной среде говорить можно только о постоянстве во времени и/или пространстве некоторой характеристики множества сигналов, отображающих информацию.

Наиболее универсальное свойство, присущее любой последовательности и в то же время индивидуальное для каждой из них, это очередность элементов (двоичных сигналов), образующих эту последовательность. Две последовательности, образованные сигналами разной физической природы, можно считать эквивалентными, если очередность элементов в одной из них такая же, как в другой. «Фиксированность» электронной информации может быть обеспечена постоянством в пространстве и во времени *очередности* сигналов, комплектующих информационную последовательность.

Понятие очередности слишком расплывчато, чтобы успешно использовать его в точной среде: надо задать начало и конец очереди, направление отсчета. А что делать, если фрагменты последовательности разбросаны в пространстве (на диске памяти) и во времени? При пакетной передаче ЭлД какой из принятых фрагментов является первым? Далеко не всегда это первый по времени, маршруты пакетов различны, и время их прибытия разное. Согласно вышесказанному, при задании на множестве информационных сигналов *бинарного отношения частичной упорядоченности* исходная последовательность однозначно восстанавливается из упорядоченных фрагментов множества.

В математике при установлении эквивалентности двух упорядоченных множеств используется термин «изоморфность». В частности, последовательность есть множество, изоморфное множеству

натуральных чисел. Логично полагать, что использование изоморфизма будет эффективно и при математическом описании информации и ее преобразований в цифровой среде. Напомним ряд математических определений [67].

Задано *отображение* F множества X **в** множество Y, если каждому элементу $x \hat{I} X$ множества X ставится в соответствие согласно правилу F элемент $F(x) = y \hat{I} Y$ и $F(X) \acute{I} Y$. Если $F(X) = Y$, то говорят, что задано отображение множества X **на** множество Y.

Взаимно однозначное отображение F частично упорядоченного множества X **на** множество Y называется *изоморфным* (*изоморфизм*), если оно сохраняет частичную упорядоченность, т. е. из $x_i \varphi x_j$, где $x_i, x_j \in X$, следует $y_i \varphi y_j$, где $y_i = F(x_i)$, $y_j = F(x_j)$, $y_i, y_j \in Y$. Сами множества X и Y при этом называются *изоморфными*.

В общем случае, когда порядок элементов множества Y определяется на основе некоторого алгоритмического преобразования порядка элементов множества X, говорят о *вычислимо изоморфном* отображении F. Обратим внимание, что здесь не предполагается взаимная однозначность отображения F и даже его однозначность. Важна лишь возможность установления (вычисления) порядка элементов любого подмножества множества Y, исходя из порядка элементов соответствующего подмножества множества X. Отметим также, что из определения не вытекает также и существование отображения F^{-1}, обратного исходному отображению F.

Понятие изоморфизма наиболее адекватно для описания информации в электронной среде: несущественен смысл информации; теряют значимость факторы времени и пространства, равно как и физической природы элементов информационного множества; установление изоморфности множеств возможно на основе логических

операций; любое преобразование реализуемо в последовательном режиме на основе фрагментации и последующей дефрагментации множества.

Отношение порядка на множестве должно быть «*задано*», а не «существовать». Любая последовательность есть множество, на котором *существует* естественное отношение порядка, но из этого не следует, что эта последовательность содержит (отображает) информацию. Из n элементов r типов можно создать r^n различных последовательностей, но только в одной из них естественное отношение порядка будет таким же, как *заданное* на исходном множестве из n элементов. Определение не требует, чтобы при отображении множества в виде последовательности естественный порядок элементов соответствовал *заданному* на множестве.

Для двоичного множества из k «единиц» и $n–k$ «нулей» существует $C(n, k)$ различных отображений в виде последовательности. Каждая может рассматриваться как содержащая одну и ту же информацию, если на последовательности *задано* соответствующее бинарное отношение упорядоченности, причем только в одном случае это отношение будет совпадать с естественным порядком элементов последовательности. Криптограмма представима в виде последовательности, естественная очередность элементов в которой не соответствует исходному порядку. Однако информация сохраняется: если отношение упорядоченности (определяемое в данном случае ключом и алгоритмом) известно, то расшифрование гарантируется.

Не требуется известности того субъекта или объекта, который *задал* отношение упорядоченности. В электронной среде это не существенно, важно только само отношение упорядоченности, которое должно «отслеживаться» программно-техническими объектами среды. Для идентификации некоторого множества сигналов как «информации» должны быть известны признаки, позволяющие объектам электронной среды распознать это множество. Для этого множество должно быть

помечено, маркировано. Конкретно способ маркировки и допустимые алгоритмы его преобразования определяются, исходя из располагаемого набора программно-технических объектов электронной среды.

Информация в электронной среде есть ***маркированное*** *детерминированным способом конечное множество (сигналов), на котором* ***задано*** *бинарное отношение (частичной) упорядоченности: для любой пары элементов множества определено предшествование одного другому.*

При электронном взаимодействии должно сохраняться отношение упорядоченности множества сигналов, маркированного как «информация», должен обеспечиваться (вычислимый) изоморфизм преобразований.

В соответствии с ГОСТом [30]: *«информация — сведения о лицах, предметах фактах, событиях, явлениях и процессах независимо от формы их представления».* Тем самым неявно подразумевается наличие интерпретатора (человека), преобразующего совокупность физических сигналов (знаков, символов) в сведение, знание. Нельзя объективный факт определять субъективными признаками: информация документа не может зависеть от его восприятия человеком.

А если такого интерпретатора нет или, например, язык неизвестен? Вытекает ли из определения, что криптограмма содержит информацию, если ключ потерян? Содержит ли она сведение или это просто «белый шум», записанный в графической форме? Аргумент, что рано или поздно криптограмму можно дешифровать, теряет силу, если на самом деле она окажется «белым шумом». Предлагаемые определения имеют смысл и в аналоговой среде, позволяя разрешить, в частности, описанный «парадокс» криптографии.

В математическом плане криптография есть вычислимо изоморфное преобразование последовательности информационных символов, а

криптоанализ есть нахождение обратного изоморфного преобразования. Информация сохраняется, хотя сведение для подавляющего большинства субъектов теряется.

2.3. Системные особенности электронного документа

2.3.1. Сектор действенности документа

Любой документ значим, действенен только при наличии конкретных социальных, экономических, технических условий, совокупность которых наблюдается, вообще говоря, не во всей среде существования, а в некоторой ее части, секторе действенности документа. Информационное взаимодействие в аналоговой среде базируется на восприятии и обработке документа мыслящими субъектами. Конструктивность взаимодействия обеспечивается системой понятий, основанных на огромном, по сравнению с ЭВМ, объеме знаний человека, накопленных им в процессе предварительного обучения и практической работы. Эти знания являются контекстом терминологии в аналоговой среде, обеспечивающим адекватное понимание терминов и понятий, трактовка которых допускает известный произвол, неоднозначность, неизбежные в силу приблизительности, похожести образного мышления.

Основной задачей документа является обеспечение правовой функции — документ признается законом или нормативно-правовыми актами как *формальное подтверждение* (юридического) факта.

Юридический факт есть предусмотренные в законе обстоятельства, при которых возникают, изменяются, прекращаются конкретные правоотношения между участниками информационного взаимодействия. По характеру последствий различают правообразующие, правопрекращающие и правоизменяющие юридические факты [7].

Строго говоря, признание того или иного факта «юридическим фактом» определяется государственными институтами. Поэтому далее будем говорить о подтверждении «*факта*», понимая последний как предусмотренные формальными и неформальными правилами, обычаями, менталитетом определенного круга субъектов обстоятельства, являющиеся формальным основанием изменений отношений между участниками взаимодействия, входящими в этот круг субъектов. Если круг субъектов есть государство, то «факт» становится «юридическим фактом». Записка с просьбой передать курьеру определенную сумму денег для доставки отправителю является достаточным основанием в рамках сложившегося коллектива, но не в рамках закона. Курьер, конечно, может утверждать, что никаких денег не получал, и закон здесь бессилен. Однако в коллективе потеря репутации курьеру обеспечена, здесь также существует определенная шкала неявных наказаний и поощрений.

Определяя правовой документ как *формальное* подтверждение факта, мы тем самым расширяем круг участников информационного взаимодействия. Помимо непосредственных участников, неявно вводится некий институт, незримо определяющий, каким требованиям должны удовлетворять содержание и атрибуты документа для того, чтобы последний считался *формальным* подтверждением. Кто-то «посторонний», существующий объективно, вне участников, должен решать, является ли данное отображение информации документом или нет. Необходим арбитр, третейский судья, занимающий более высокий уровень иерархии по отношению к участникам взаимодействия и решающий в спорных ситуациях, какое конкретно сведение содержится в данном документе. Подобная предпосылка неявно просматривается и в работах других авторов, например, в работах [68, 69] вводится «надсистема» документа, понятие, где-то эквивалентное сектору действенности.

Арбитр должен иметь право и возможность воздействия на участников спора, поощряя их действия в случае «правильной» трактовки документа и наказывая за ошибочную интерпретацию. Воздействие обеспечивается обществом, точнее его частью — сектором действенности документа. Для этого в секторе имеются соответствующие институты: взаимное недовольство, если документ — частное письмо; низкая оценка на экзамене, когда документ — учебник; выговор или лишение премии, если документ — распоряжение руководства фирмы; гражданская, административная или уголовная ответственность, когда сектор действенности документа есть государство.

Можно ли считать таким арбитром всю среду существования аналогового документа, устанавливающую правила обработки, хранения и передачи информации, представленной в образной форме? Специфика документов настолько различна, что в общем случае это невозможно. А вот некоторую, соответствующим образом специализированную для данного класса документов, часть среды существования — можно. Приходим к понятию *сектора действенности документа*. Именно в адекватном документу секторе действенности реализуется назначение документа: элементам сектора, участникам информационного взаимодействия, предоставляются в соответствии с содержанием документа права и/или налагаются обязанности.

Понятие документ имеет смысл только при явном или неявном задании его сектора действенности. *Документ определяется как пара: сектор действенности и информация, оформленная в соответствии с правилами сектора действенности.*

Сектор действенности аналогового документа — максимальное замкнутое подмножество элементов (субъектов) среды существования, характеризующееся едиными, обязательными для всех его субъектов, явными и неявными правилами оформления документа и трактовки прав и

обязанностей, которые предоставляются и/или налагаются таким документом на участников информационного взаимодействия.

В рамках сектора действенности документ признается формальным подтверждением факта как основаниея для возникновения, изменения, прекращения конкретных отношений между элементами сектора — субъектами/объектами информационного взаимодействия.

Разобравшись с аналоговой средой, можно перейти к электронной и рассмотреть понятие *сектора действенности электронного документа*. При этом рассматриваются только *прямые* участники электронного взаимодействия, объекты электронной среды, реализующие *собственно* процессы обработки и преобразования ЭлД. Подмножество электронной среды образуется некоторой совокупностью программно-технических средств вычислительной техники. Замкнутость означает, что эти средства объединены в единое целое, представляют собой изолированную информационно-вычислительную систему или подсистему, за пределы которой электронный документ не выходит. Можно построить иерархию секторов действенности ЭлД. Например, папка «мои документы», персональный компьютер, локальная подсистема корпоративной системы, корпоративная система, совокупность систем и т. д.

Правами и обязанностями неодушевленные объекты обладать не могут, но можно говорить о возможностях и ограничениях, накладываемых сектором действенности на его компоненты. Точно так же как и в аналоговой среде, эти возможности и ограничения определяются «внешней силой» относительно объектов сектора действенности ЭлД. Но здесь эту роль играет не общество, как ранее, а субъект, определяющий состав и конфигурацию инструментальных средств, программно-техническую базу, правила доступа, алгоритмы и дисциплину формирования, обработки, передачи и хранения ЭлД в системе.

Прямыми участниками электронного взаимодействия являются неодушевленные объекты сектора, но не субъекты, находящиеся вне сектора действенности ЭлД. По существу, мы имеем определенное подобие электронного и аналогового секторов действенности. Некоторый произвол, разрешаемый субъектам аналогового сектора, не является индикатором качественных отличий от ограничений на действия объектов сектора действенности ЭлД. При ближайшем рассмотрении «свобода» в аналоговой среде не столь уж и велика. Например, распоряжение прибыть к 17^{00} устанавливает диапазон безнаказанности буквально в несколько минут, хотя прямо и не указано, что подразумевается местное время, а не, например, гринвичское.

В соответствии с заложенными «свыше» правилами (алгоритмом), объект (программно-технический модуль) электронного сектора извлекает из цифрового множества, отображающего поступивший ЭлД, нужное подмножество, определяет требуемое преобразование, выполняет, формирует выходной ЭлД и отправляет по назначению другому объекту данного сектора действенности ЭлД. Если в процессе обработки должен участвовать субъект аналоговой среды, то объект электронной среды формирует соответствующий ЭлД, который доставляется в рамках сектора к обратной стороне экрана монитора, возбуждает люминофор и отображается на внешней стороне в виде аналогового документа. Далее все операции производятся по правилам аналоговой среды. После выработки субъектом решения он формирует электронный документ-команду, вводит его в сектор действенности, и далее система на основе исходного ЭлД и ЭлД-команды выполняет предписанные действия.

Можно отметить только одно существенное отличие аналогового и электронного секторов действенности. В аналоговом секторе правила трактовки и обработки документа могут вырабатываться как вне, так и в рамках сектора, самими субъектами, всеми или частью. После чего эти

правила доводятся до сведения остальных членов сектора, в том числе и не принимавших участие в разработке. В электронном секторе правила (алгоритмы) трактовки ЭлД детерминированы, определяются обязательно вне рамок сектора, но точно также доводятся «до сведения» его программно-технических объектов. Это отличие не является принципиальным, на момент обработки документа правила всегда фиксированы, а уж кто и как их выработал, не имеет значения.

Сектор действенности электронного документа — максимальное замкнутое подмножество элементов (программно-технических объектов) среды существования ЭлД, характеризующееся едиными, обязательными для всех его элементов, детерминированными правилами (алгоритмами), определяющими возможности и ограничения обработки и преобразования документа в зависимости от вида отображающего его цифрового множества.

Электронный документ есть информация, *оформление* которой признается определенным сектором электронной среды существования достаточным для признания ее *фактом — основанием для возникновения, изменения, прекращения конкретных взаимодействий (процессов) между программно-техническими объектами сектора среды*.

В общем случае возможно разбиение сектора действенности электронного документа на подсектора, являющиеся замкнутыми подмножествами элементов сектора с едиными в пределах подсектора правилами обработки и преобразования документа. Эти правила должны быть непрерывными на границах, интерфейсы электронных устройств должны быть совместимыми. Так как документ реализует свое назначение только в рамках сектора (подсектора) действенности, то требования к его компонентам, содержанию и оформлению определяются сектором. Естественно, что задачи и интересы *(под)сектора* действенности не должны противоречить законам и правилам, установленным в более

широком секторе и среде в целом. Сектор действенности есть только часть, но не вся среда существования документа. Но это проблема сектора, а не документа. Фигурально выражаясь, существует только один «хозяин», диктующий правила интерпретации и оформления документа, сектор действенности документа.

2.3.2. Содержание и атрибуты документа

Многообразие сущности, смысла документированной информации априорно допускает только самую общую регламентацию ее конкретного отображения в виде содержания документа: профессионально ориентированная тематика, язык, объем, стиль изложения, правописание и др. Это сравнительно размытые требования, их выполнение на приемлемом уровне возможно только человеком. Поэтому обычно при создании электронного документа приходится вначале формировать содержание документа в аналоговой среде, а затем отображать содержание в составе электронного документа, используя интерфейс между средами.

Но для узкоспециализированных документов, с условно постоянным содержанием, требования к содержанию могут быть сформулированы точно, что сразу обусловливает возможность их выполнения в рамках электронной среды. К таким документам принадлежит подавляющее большинство коммерческих документов, и здесь преимущества ЭлД по сравнению с АнД наиболее существенны.

Оформление документа обеспечивается совокупностью признаков (атрибутов), в достаточно широких пределах не зависящих от содержания документа, для каждого класса документов оформление постоянно. Поэтому на атрибуты документа возлагается решающая роль при обеспечении служебных функций, необходимых для признания документа в рамках сектора действенности как юридического факта. Для этого

оформление документа должно соответствовать определенным требованиям сектора: как явным, выраженным в соответствующих нормативно-правовых актах, действующих в секторе, так и неявным, подразумеваемым правилами и обычаями, устоявшимися в секторе.

Атрибуты документа должны предусматривать выполнение приводимых далее требований в общем случае, но не всегда: зачастую необходимо обеспечение лишь части требований. «Предусматривать» выполнение, но не «выполнять» — достаточно часто для этого необходима определенная инфраструктура. Например, для банкноты не требуется конфиденциальность, но для индикации подлинности (аутентификации автора) банкноты требуется специальное оборудование. Ниже приводится максимальный набор требований, не все из них обязательны для документов различного назначения.

1. Возможность индикации *целостности*.

Мы говорим именно об *индикации*, но не об обеспечении целостности, хотя и та, и другая функция сильно переплетаются. Целостность понимается как отсутствие в содержании документа купюр, искажений или модификаций. В аналоговом документе, написанном чернилами на рыхлой (промокательной) бумаге, целостность хорошо *индицируется* — трудно незаметно «подчистить» такой документ, не повредив носитель. Но плохо *обеспечивается* — непрочный носитель легко повреждается. В практических приложениях приходится идти на определенный компромисс, но свойство индикации должно превалировать: как правило, отсутствие информации — предпочтительнее ложной информации.

Должен существовать некий индикатор целостности, неразрывно связанный с содержанием документа, так что любая модификация содержания изменяет состояние индикатора. В аналоговой среде в качестве индикатора используются свойства носителя документа,

бумажного листа, а в качестве «клея» для графического отображения информационных символов — способ нанесения символов на носитель. В электронной среде, как было показано выше, носитель активного ЭлД принципиально не может быть зафиксирован. Остается единственный класс методов — задание некоторой функциональной зависимости на множестве чисел, элементов содержания, и последующая индикация (проверка) выполнения этой зависимости.

Принципиальная трудность заключается в том, что либо сама зависимость, либо значение функции должны быть априорно известны всем участникам электронного взаимодействия. А значит, не исключается, что и нежелательным третьим лицам, намеренно нарушающим целостность документа.

2. *Доступность* содержания документа субъектам/объектам сектора действенности.

Способ отображения информации должен соответствовать действующим в рамках сектора стандартам и сложившимся неформальным правилам, обеспечивающим единство восприятия и обработки документа субъектами сектора. Например, письмо российской организации в профильное министерство должно быть на русском языке, на белой плотной бумаге, с полями, напечатано шрифтом определенного размера и т. д. Для аналогового документа такое требование настолько естественно, что о нем даже не упоминают. Для электронного документа доступность является существенным фактором. Необходимо соблюдение единых стандартов отображения документа в цифровом виде, либо наличие соответствующих конвертеров, обеспечивающих совместимость различных стандартов.

3. *Недоступность* содержания документа субъектам/объектам иных, априорно заданных, секторов действенности *(конфиденциальность).*

В предыдущей позиции говорится о доступности только субъектам сектора действенности адресата документа, но не других секторов. Но единство стандартов как раз предполагает доступность документа всем элементам среды, применяющих данные стандарты. Достаточно часто возникает задача сохранения в тайне содержания документа, а зачастую — и самого существования документа, от заранее очерченного круга лиц или объектов среды. Такое свойство называют *конфиденциальностью* документа.

Круг нежелательных объектов может задаваться с произвольной точностью. Достаточно часто конфиденциальность понимают как недоступность содержания документа всем субъектам (объектам) аналоговой (электронной) среды, кроме субъектов, принадлежащих сектору адресата [70]. Это явно завышенное требование, многократно увеличивающее затраты ресурсов на обеспечение конфиденциальности. Неразумно шифровать коммерческую переписку, исходя из арсенала возможных средств дешифровки спецслужб государств, достаточно, чтобы не могли узнать содержание коммерческие конкуренты.

4. Возможность *аутентификации автора* и/или отправителя документа.

Надо «привязать» документ как предмет, вещь, к субъектам, существующим независимо и вне документа, т. е. аутентифицировать документ.

Аутентификация документа — объективное подтверждение содержащейся в нем идентифицирующей информации.

Когда говорят, что требуется идентифицировать автора документа, фактически подразумевают аутентификацию документа. Автор — это не документ, это субъект, человек. Идентифицировать автора X документа означает, что из нескольких поставленных рядом людей, пусть X, Y, Z, надо узнать, кто именно подписал документ, кто из них X. Тогда как в

действительности требуется установить, что подпись (идентифицирующаяся информация) человека, поименованного в документе как X, действительно принадлежит X .

5. Возможность *аутентификации получателя* и/или адресата документа.

Взаимодействие предполагает наличие не менее двух участников. Часто необходимо подтверждение не только отправителя, но и получателя документа: если отсутствует подтверждение в получении документа, последний не признается сектором действенности в качестве такового. И часто даже, наоборот, не требуется аутентификация отправителя документа, но обязательно — получателя; например, взнос (пожертвование) в партийный фонд, или анонимный платеж в счет погашения долга субъекта X субъекту Y. Так что в общем случае оформление документа должно предусматривать возможность аутентификации всех участников информационного взаимодействия.

Здесь также сохраняет справедливость замечание из предыдущей позиции об аутентификации объекта электронной среды.

6. Возможность *аутентификации маршрута* (промежуточных точек) прохождения документа от отправителя до получателя.

В общем случае существенно не только, кто документ отправил и кто получил. Например, правительственный документ, принесенный посторонним прохожим, а не доставленный курьером или спецпочтой, не будет признан документом без дополнительной проверки. Поэтому оформление должно предусматривать, в соответствии с требованиями сектора действенности, возможность аутентификации промежуточных инстанций передачи и обработки документа от автора до адресата.

При электронном взаимодействии проблема аутентификации маршрута ЭлД принципиально намного острее: в силу возможности удаленного доступа потенциальное число субъектов (объектов), которые

могут взаимодействовать с электронным документом на маршруте его прохождения, многократно превышает такое же для АнД. В ответственных ситуациях может потребоваться не только аутентификация субъектов аналоговой среды, но и объектов электронной среды, программно-технических устройств, использованных в процессе формирования, обработки и передачи электронного документа.

7. Возможность *кратного применения* документа.

В аналоговой среде эквивалентные реализации различимы, так что обеспечение уникальности экземпляра средствами оформления документа в принципе достижимо. Любая из реализаций одного аналогового документа отличается от любой реализации другого, и с этой точки зрения АнД необходимо уникальны. Если эквивалентные реализации одного и того же документа различимы по какому-либо второстепенному параметру, не входящему в число признаков эквивалентности, то в зависимости от степени различий можно говорить об идентичных документах или о разных экземплярах АнД.

Для того чтобы являться правовым основанием действий участников информационного взаимодействия, необходимо физическое наличие документа кратного действия, его передача от одного участника другому. При использовании они фактически потребляются, иначе — зачем требовать их наличие. Любое потребление изнашивает документ, через конечное число актов документ приходит в негодность, что и обусловливает возможность только конечного числа их применения, поэтому подобные документы также называются «потребляемыми». Кассовый чек, билет на самолет являются документами однократного действия, проездной абонемент, банкнота, вексель — кратного. После совершения правового действия (обмена чека на товар, проезда, оплаты) потребляемый документ или аннулируется (погашается), или передается правопреемнику, или меняет свойства. Здесь необходима не только

подлинность реализации (экземпляра), но и ее уникальность, чтобы множество реализаций документа состояло всего из одного элемента.

Документы неограниченного действия или непотребляемые документы при использовании не теряют существенных первоначальных свойств. Для выполнения функции правового основания достаточен только факт существования, но не наличие документа, тем более — передача документа от одного участника другому. Например, федеральный закон, Конституция страны, диплом об образовании и т. п. Для подобных документов требование уникальности реализации не является существенным. Любой из экземпляров (реализаций) тиража официальной публикации аналогового документа имеет одинаковую юридическую силу.

2.3.3. Электронный документ как множество неразличимых реализаций

Органически присущее аналоговой среде свойство «похожести» сразу влечет потребность в ее измерении, хотя бы на качественном уровне. По существу, именно такая качественная оценка близости двух традиционных документов дается понятиями «аналогичные», «эквивалентные», «одинаковые», «идентичные» документы. Однако перенос подобных терминов на электронную среду, применительно к электронному документу, вызывает сомнения: выше установлено, что это среда точная. Требуется более тщательный анализ.

Математика отражает, пусть идеализировано, процессы и явления реальной жизни. Рассматривая идентичные документы, мы тем самым неявно выделяем множество документов, отличие между которыми незначительно, документы «близки», «расстояние» между ними очень мало. Фактически на множестве документов X задается некоторая мера, называемая «расстоянием», которую для практических целей можно трактовать, например, как степень «похожести» документов. Само

множество с определенным расстоянием называют метрическим пространством.

Метрическим пространством называется пара (X, ρ), состоящая из некоторого множества (пространства) X элементов (точек) и расстояния, т. е. однозначной, неотрицательной, действительной функции $\rho(a, b)$, определенной для любой пары $a, b \in X$ элементов множества X.

Эта функция может быть выбрана в достаточно широком диапазоне, но не произвольно: должны выполняться так называемые аксиомы метрического пространства:

- $\rho(a, b) = 0$ тогда и только тогда, когда $a = b$;
- (аксиома симметрии): $\rho(a, b) = \rho(b, a)$;
- (аксиома треугольника): $\rho(a, c) \le \rho(a, b) + \rho(b, c)$, где $a, b, c \hat{I} X$.

Любые два элемента a, b из X являются разными или *различимыми*, если расстояние между ними отлично от нуля, $\rho(a, b) \neq 0$. Элементы a, b из X являются одинаковыми (идентичными, тождественными) или *неразличимыми*, если расстояние между ними равно нулю, $\rho(a, b) = 0$. Любой из неразличимых элементов полностью характеризует все остальные, следовательно, — и все множество. Множество неразличимых элементов может быть идентифицировано на основе любого подмножества своих элементов: для индикации жидкости в стакане достаточно любой капли.

Структурные свойства множеств, образованных неразличимыми и различимыми элементами, могут отличаться кардинально. Например, из n *различимых* (разных) элементов можно сделать $n! = n(n–1)(n–2)\ldots2\cdot1$ разных перестановок, тогда как из n *неразличимых* (одинаковых) всего одну. (Для $n = 10$ соотношение 3 628 800 к 1.)

Этот небольшой экскурс в арифметику иллюстрирует важность фактора различимости при анализе свойств множеств. Объединение

объектов во множество по умолчанию всегда означает, что они в каком-то смысле «одинаковы», эквивалентны: характеризуются некоторым набором одинаковых характеристик, называемым «отношением эквивалентности». Отношение эквивалентности (обозначим его ≡) можно выбрать в очень широком диапазоне, но не произвольно: оно должно удовлетворять определенным ограничениям:

- (аксиома рефлексивности): $a \equiv a$;
- (аксиома симметричности): если $a \equiv b$, то $b \equiv a$;
- (аксиома транзитивности): если $a \equiv b$ и $b \equiv c$, то $a \equiv c$.

Если объекты множества характеризуются *только* отношением эквивалентности, то они *неразличимы* — отсутствуют параметры, позволяющие выделить один из них относительно другого. Тогда сама постановка вопроса об *отдельном* элементе множества абсурдна, можно говорить только о *любом* элементе. Для того чтобы выделить объект, его надо как-то пометить, объект должен отличаться от других, но это невозможно, так как по исходному предположению любой объект имеет один и тот же набор характеристик.

Таким образом, на практике выделение наперед заданной произвольной реализации электронного документа невозможно. В каком-то смысле реализация ЭлД подобна молекуле вещества. Для исследования свойств вещества достаточно любой молекулы, все остальные точно такие же (неразличимость молекул). Для восприятия документа достаточно любой его реализации.

Для того чтобы измерения воспроизводились, приходится защищать (например, от окисления) все вещество, все его молекулы, поскольку неизвестно, какие конкретно молекулы будут использованы в повторном опыте. Для защиты электронного документа приходится защищать среду существования, тем самым защищаются все возможные реализации, которые могут быть созданы.

Свойство неразличимости молекул вещества не удивляет, тогда как постулат неразличимости реализаций электронного документа вызывает внутренний протест: положения цитированных в гл. 1 законов достаточно иллюстративны. Целесообразно отказаться от принципа различимости отдельных реализаций ЭлД и считать, что *электронный документ есть множество неразличимых реализаций*. С целью подчеркнуть отличие от понятий традиционного документооборота, здесь говорится о *реализациях*, но не об *экземплярах* ЭлД.

Существует только один, единственный электронный документ, единственная, с точностью до изоморфизма, последовательность двоичных сигналов.

Проблема практического использования электронного документа должна решаться исходя из существования множества эквивалентных реализаций. *Юридическую силу имеет только собственно документ, понимаемый как множество реализаций*. Для документов многократного действия (например Федеральный Закон) достаточно доказать существование множества, что возможно на основе единственной реализации ЭлД, имеющей соответствующие атрибуты. Для документов однократного (например, электронное платежное поручение) или кратного (электронный билет в метро) действия дополнительно к указанным характеристикам необходимо еще гарантировать кратность применения данного ЭлД. Например, ограничить срок действия документа и логически отслеживать кратность регистрации его реализаций в течение срока его действия.

2.3.4. «Оригинал», «копия», «экземпляр» документа в электронной среде

На практике, кроме единого для всех объектов множества признаков эквивалентности, объекты могут обладать и рядом несовпадающих признаков. Можно построить иерархию признаков эквивалентности, начиная от общего и переходя к более детальным, постоянным признакам в рамках отдельных подмножеств. Объекты являются *различимыми*, если иерархия признаков эквивалентности позволяет дойти до подмножеств, состоящих всего лишь из одного объекта. Только тогда объекты можно выделить и сравнить между собой, только тогда можно говорить об *экземпляре* объекта, обладающего общим признаком эквивалентности. Если не удается вычленить каждый объект, то приходим к предыдущей ситуации на уровне подмножества — неразличимости входящих в него объектов.

Сопоставление двух документов или документа и эталона неявно предполагает их различимость: документы имеют одинаковые признаки высокого уровня (пусть, содержание), но отличаются признаками эквивалентности более низкого уровня (пусть, координаты листа бумаги). Как ни парадоксально, но абсолютно верной является следующая фраза: — «Два *разных* документа являются *одинаковыми*, идентичными, если … (далее условие идентичности)». Когда объекты *неразличимы*, то говорить об их идентичности, одинаковости, не имеет смысла: это один и тот же объект.

Понятия «идентичные, одинаковые документы, экземпляры документа» имеют смысл тогда и только тогда, когда индицируется признак, позволяющий различать один документ (экземпляр) от другого: когда документы различимы.

Аналоговый документ отображается информационным множеством бесконечной мощности. При этом для описания содержания документа достаточно, в принципе, конечного подмножества: хотя символ-буква есть бесконечное число точек, но значение символа единственно — его

наименование. А вот атрибуты аналогового документа отображаются бесконечным подмножеством. Точно воспроизвести бесконечное множество за конечное время нельзя, поэтому любые два аналоговых документа принципиально различимы.

Различение и распознавание (т. е. классификация) документа далеко не одно и то же. Классификация подразумевает выявление совпадения (равенства) признаков эквивалентности заданного уровня у рассматриваемого документа с такими же — у эталона. Это могут быть признаки различного уровня: визуального контроля, приборного, криминалистического и т. д. При совпадении признаков эквивалентности вплоть до некоторого уровня говорят об *одинаковых или идентичных* документах. Если документы различимы, то классификация позволяет дойти до отдельного документа.

Обычно, говоря об *одинаковых* АнД, понимают эквивалентность отражающих их содержание *конечных* подмножеств значений информационных символов. При одинаковом содержании атрибуты могут быть совершенно разными: один документ — рукописный, другой — машинописный. Расширяя эквивалентные подмножества включением информационных атрибутов, части материальных атрибутов (шрифт, плотность и размер бумаги) усиливают понятие одинаковости, и, начиная с некоторого момента, называют такие документы идентичными.

Использование терминов «одинаковый», «идентичный», «экземпляр» для АнД оправдано образным восприятием человека и ярко выраженной вещной стороной АнД. Человек, основываясь на контексте взаимодействия, обычно правильно интерпретирует термины: это может быть тождественное содержание, часто дополнительно требуется совпадение некоторых реквизитов, а иногда достаточно лишь одинакового «смысла» документов. В силу присущей аналоговой среде

«приблизительности» критерии идентичности, одинаковости, экземпляра документа задаются достаточно расплывчато.

В аналоговой среде различимость идентичных документов подразумевается по умолчанию, на основе очевидных физических признаков: местоположение в пространстве, графическое отображение информационных символов, свойства носителя и т. п. Все это — характеристики атрибутов АнД. Детализируя описание атрибутов, в конце концов, приходим к несовпадающим характеристикам. Для АнД на твердом носителе (листе бумаги) всегда существует хотя бы один признак, хорошо различимый для двух документов: координаты носителя в пространстве. Аналоговые документы — принципиально различимые документы.

Специфика электронной среды приводит к проблематичности решения задачи различимости отдельных реализаций ЭлД: индикация признаков эквивалентности нижних уровней иерархии требует неоправданно высоких затрат и чаще всего практически нереальна. Как установлено ранее, в отличие от аналогового документа, существующего только в статической форме, электронный документ существует в двух формах: как явление — в статической форме в пассивном состоянии (при хранении); как процесс — в динамической форме в активном состоянии (при обработке, передаче, визуализации). Статические явления поддаются анализу намного легче, чем динамические. Если различимость статических реализаций интуитивно ясна, то различимость процессов требует разработки конкретной для каждого процесса системы сравнения.

Можно, конечно, идентифицировать динамическое явление, процесс, по его статическим — начальной и конечной — точкам. Но чаще всего сам процесс носит циклический характер, так что понятия начала и конца, в свою очередь, весьма условны. Органически присущий электронной среде механизм копирования позволяет технологически просто создавать новые,

тождественные (с точностью до элемента или устройства) реализации на основе исходной. Физическая природа реализаций может кардинально отличаться: ориентация доменов на магнитном диске, свечение люминофора на экране, потенциальные уровни элементов микросхем, способ модуляции радиосигнала и т. д. При активизации ЭлД время жизни почти всех его реализаций ничтожно, доли микросекунды.

Электронная среда есть среда логических операций. Любая логическая операция над двумя разными, но изоморфными множествами ведет к одному и тому же результату, эти множества в цифровой среде *эквивалентны.* В каком-то смысле изоморфность подобна изменению обозначений аргумента функции. С таким же успехом можно было бы говорить, что функция $F(x)$ существует в нескольких экземплярах — $F(y)$, $F(z)$, $F(t)$, и что каждый из них равносилен $F(x)$. Понятие «экземпляр ЭлД» в цифровой среде имеет столько же смысла, сколько «экземпляр функции». Когда говорят о двух экземплярах ЭлД на разных дискетах, то подразумевают два экземпляра дискет, но не документа. Электронный документ один — фиксированный порядок двоичных сигналов. Нельзя называть экземплярами человека его отражения в поставленных под углом зеркалах.

Множество атрибутов ЭлД, характеризующих различные реализации документа, имеет конечную мощность, так что ресурсы для создания различных атрибутов «идентичных» документов намного скромнее, чем в аналоговом случае. Пространственные координаты документов есть характеристика аналогового мира, там для каждого предмета можно указать достаточно точное положение. Физические координаты размещения реализаций ЭлД известны с большой неопределенностью, в лучшем случае — с точностью до устройства, диска, дискеты, оперативной памяти. Где-то на диске расположен данный ЭлД, причем его фрагменты рассеяны по всему диску.

Один и тот же документ может быть представлен на диске в нескольких эквивалентных реализациях (.doc, .txt и т. п.).

Эти *реализации эквивалентны*: существует детерминированная вычислительная процедура, преобразующая одну реализацию ЭлД в другую. В общем случае надо говорить об *эквивалентных*, а не о неразличимых или тождественных реализациях ЭлД. Современные программно-технические средства предоставляют очень широкие возможности обратимых преобразований, сохраняющих все особенности документа. Это означает, что на практике всегда имеется такой набор программных и технических средств, который позволит преобразовать любую реализацию ЭлД в одну и ту же наперед заданную форму представления документа.

На практике понятие «экземпляр» настолько устоялось, что воспринимается самостоятельно, о множестве забывают. В обыденной жизни «экземпляр» ассоциируется с некоторым отдельным предметом, зафиксированным в пространстве. Два «экземпляра» означает, что два предмета, координаты которых в пространстве известны с достаточной точностью, характеризуются одним и тем же набором равных по величине параметров. Местоположение реализаций ЭлД известны с большой погрешностью, и здесь, в отличие от двух разных экземпляров АнД, отличить один «экземпляр» от другого обычно невозможно.

Воспользуемся известной ассоциацией с водой. Вещество и его молекула все-таки понимаются по-разному: молекула воды состоит из атомов водорода и кислорода, но вода не является смесью этих веществ, это другое качество. Вода — жидкое вещество, а вот про ее молекулы этого не скажешь. Документ как множество — это не механическая смесь его реализаций (пусть даже — экземпляров), это качественно иной объект. Защищать надо *множество* реализаций, а не каждую; юридическую силу имеет *множество*, а не отдельный «экземпляр» электронного документа.

Другое дело, что свойства множества могут быть определены на основе одной или нескольких реализаций, но это свойства *множества*, а не *реализации*.

Разумеется, полученный результат вытекает из свойств электронной среды, где возможны только точные результаты: либо «да», либо «нет». Любые две реализации ЭлД либо эквивалентны — и тогда это один и тот же документ, либо нет — и тогда это разные документы (два одинаковых текста, отличающиеся одним пробелом, воспринимаются ЭВМ как разные документы). Принятие постулата «*электронный документ есть множество эквивалентных реализаций*» позволяет избежать парадоксов, присущих обыденной терминологии электронного взаимодействия.

Количество реализаций (мощность множества) не лимитируется, более того, может меняться в зависимости от времени и способа отображения. Например, в режиме хранения можно говорить о единственной реализации на диске; в режиме активизации — о нескольких: на диске, в оперативной памяти, в памяти видеокарты, на мониторе и др.

Идентификация собственно ЭлД, т. е. множества реализаций, возможна на основе его некоторого подмножества, вплоть до одной реализации. Можно идентифицировать ЭлД по первой полученной реализации, или на основе мажоритарной логики, или по реализации, полученной в заданном временном диапазоне, и т. д.

Из интерпретации электронного документа в виде множества неразличимых реализаций логично вытекает естественное для документа свойство уникальности. Хотелось бы отделить уникальность документа от уникальности экземпляра документа — в аналоговой среде эти два различных понятия зачастую смешиваются. Уникальность документа есть функциональное свойство: существует одна и только одна Конституция страны, одни и только одни правила дорожного движения (ПДД), одна и

только одна денежная купюра с данным номером, и т. д., и т. п. И это свойство любого документа, в противном случае конфликт неизбежен. Уникальность экземпляра есть свойство технологической реализации отображения документа, иногда это свойство необходимо (денежная купюра), иногда — нет (ПДД).

В аналоговой среде субъектов такое смешивание обычно не ведет к противоречиям, по контексту применения субъекты разделяют понятия. В электронной среде компьютер контекст применения не воспринимает, и допущение нескольких «одинаковых экземпляров» ЭлД, каждый из которых имеет «одинаковую юридическую силу», ведет к катастрофе. В любой момент времени существует один и только один ЭлД с данными параметрами — любой электронный документ уникален.

Какие параметры выбрать для обеспечения уникальности, решают специалисты в зависимости от конкретных условий реализации электронного взаимодействия. Важно отметить, что практические способы существуют: например, в рамках одной машины можно использовать электронный адрес; в рамках информационной системы — значение хэш-функции.

Применительно к электронному документу теряют содержательный смысл понятия «идентичные», «одинаковые», «экземпляры». Подобные категории, как было показано, предполагают *совпадение заданных в явном виде* одних параметров сопоставляемых документов и индицируемое элементом среды (субъектом) некоторое отличие других параметров, заданных *неявно*, контекстом. Объект электронной среды может индицировать только явно заданные параметры: но если все параметры совпадают с эталоном (эквивалентные реализации ЭлД-множества), то это не «идентичный» ЭлД, а «тот же самый» ЭлД; если нет (не эквивалентные реализации) — то это другой ЭлД, не имеющий, в общем случае, никакого отношения к эталону.

Разумеется, использование терминов допустимо просто как обозначение взаимосвязи двух различных документов или двух реализаций одного и того же ЭлД: выбор обозначений произволен. Например, две записи ЭлД на различных дискетах надо трактовать как *один и тот же* документ, а не как два «идентичных» ЭлД: для машины эти записи *неразличимы*. Но не для человека, вставляющего дискеты в дисковод: в аналоговой среде дискеты различимы, хотя сами записи неразличимы машиной.

Рассмотренные ранее государственные законы и законопроекты предписывают считать все «идентичные экземпляры» ЭлД подлинниками и гарантируют равную юридическую силу каждого. К каким казусам приводят подобные законы, было показано на примере неограниченного числа выплат по одному и тому же электронному платежному требованию, мультиплицированных на соответствующей автоматизированной системе. При традиционном подходе к *электронному* документу с позиций *аналогового* восприятия парадокс неизбежен.

Но если опираться на установленные положения, то все становится на свои места. Коль скоро электронный документ есть *множество*, то задача индикации ЭлД сводится к задаче индикации *множества*. Множество из неразличимых элементов (реализаций) индицируется любым его представителем: элементы неотличимы, так что всю информацию о каждом элементе, т. е. о множестве в целом, можно получить на основе любого элемента (реализации). Сколько бы элементов множества мы ни индицировали, это будет то же самое множество, тот же самый электронный документ. Тогда дублирование на разных дискетах платежного поручения дает право только на единственную выплату, ведь сам документ (множество) единственен. Решение задачи обеспечения заданной кратности применения ЭлД должно производиться на «приемном

конце», на этапе индикации, но не на этапе создания. На практике, разумеется, так и делается, хотя закон и нацеливает на обратное видение.

Изображение электронного документа на экране монитора меняется десятки раз в секунду, каждый кадр есть одна из реализаций ЭлД-множества. Реализации неразличимы, и их совокупность является одним электронным документом. При традиционном подходе мы имели бы дело с неопределенным числом «экземпляров» электронного документа, каждый из которых, кстати говоря, чисто физиологически не воспринимается человеком. О каком качестве решения можно говорить, если оно принимается на основе просмотра 1000 «экземпляров» документа (примерно 40 секунд экранного времени), и в каждом экземпляре воспринято несколько букв. Для аналогового документа это бессмысленно, но для электронного почему-то считается допустимым.

Находит логическое объяснение специфика защиты электронной информации. Буквально трактуя традиционный подход, достаточно было бы защитить «экземпляр-подлинник», например, зашифровать его на диске памяти. Но как тогда работать, ведь активизация документа неминуемо ведет к созданию новых реализаций, которые, в принципе, могут быть искажены путем несанкционированного доступа к ним. Что из того, что на диске подлинник, если на экране его искаженное изображение. Надо защищать и реализации. Здесь мы сталкиваемся еще с одним проявлением взаимообусловленности свойств ЭлД: статический и динамический характер существования ЭлД обусловливает и столь же кардинальное различие методов его защиты: защита собственно документа и защита среды его существования, образуемой инструментальными средствами вычислительной техники, создание адекватных технологий обработки ЭлД.

Предлагаемая интерпретация ЭлД как множества реализаций сразу доказывает недостаточность защиты только документа или каждой его

реализации. Локализация реализаций ЭлД в машине меняется во времени, даже в один и тот же момент в ЭВМ может находиться несколько реализаций (на диске, в оперативной памяти, в арифметических устройствах и т. д., и т. п.). Технически много проще защитить от несанкционированного доступа среду, чем определить те точки и те моменты времени, где и когда может находиться каждая реализация ЭлД.

В аналоговом мире понятия *оригинал и копия* достаточно различимы. Копия «очень похожа» на оригинал, но имеет отличие, индицируемое субъектами взаимодействия. В мире приблизительности такое разделение имеет право на существование. Конечно, копия документа — это тоже документ, но «второго сорта», нечто похожее на оригинал, имеющее то же самое содержание, но иные атрибуты. Например, отсутствует истинная подпись и печать автора, но есть соответствующие атрибуты и реквизиты нотариуса.

Определение информации в электронной среде как конечного упорядоченного множества автоматически означает возможность его (множества) изоморфного отображения в другое множество. Можно ли назвать это другое множество копией первого? В обыденном смысле, копия — это «очень похожий» объект, но все-таки чем-то отличающийся от исходного. В точной среде нет понятия «похожести», есть только «равно или не равно», «да» или «нет». Электронные цифровые подписи (ЭЦП) двух ЭлД, отличающихся только одним пробелом, несопоставимы. Если «копия» ЭлД изоморфна оригиналу, то это не «копия», а «тот же самый документ», если нет — то «совершенно другой», и, значит, не копия. В аналоговой среде слово «докум,ент» можно рассматривать как копию (пусть, плохую) слова «документ», в цифровой среде число 12345678 нельзя считать копией числа 12345,678, хотя уровень «похожести» такой же. В электронной среде понятие «копия ЭлД» не имеет, строго говоря, содержательного смысла.

В электронной среде существует единственная альтернатива: либо «точно то же самое», либо «абсолютно другое». Но тогда становится бессмысленной аналоговая трактовка копии документа, как нечто сильно «похожее» на оригинал, но не «точно» оригинал. Для ЭВМ это либо абсолютно разные объекты, даже если отличие ничтожно, либо одно и то же. Так как двух оригиналов не может быть по определению, то можно говорить только о новом документе с таким же содержанием. Поэтому далее мы будем говорить о документе–оригинале и о документе–копии.

Положение, что электронный документ есть множество неразличимых эквивалентных реализаций, делает значимой проблему существования копий ЭлД. В самом деле, нужна ли копия ЭлД, если можно воспользоваться реализацией оригинала? На первый взгляд ответ очевиден: оригинал всегда предпочтительней копии, так что копия ЭлД не нужна. Такой подход и развивается в законодательных документах государственного уровня, явно или неявно декларирующих отказ от копий ЭлД. Многочисленные примеры рассмотрены в Главе 1. Там же была показана и абсурдность подобных предписаний, не учитывающих ряд специфических особенностей электронного документа.

Для обоснования необходимости существования электронных копий ЭлД ограничимся только парой причин, хотя, несомненно, их количество больше. Первая причина — моральное старение электронного документа, здесь подразумевается не содержание, но атрибуты ЭлД. Для аутентификации ЭлД используются средства с конечным сроком действия, например, электронная цифровая подпись (ЭЦП), коды аутентификации и др. Периодически эти средства обновляются, так что спустя конечное время контроль ЭЦП становится невозможным: ключи, хранимые отдельно от документа, оказываются уничтоженными. Такое характерно, как правило, для документов неограниченного действия, например, законодательный акт, внутрифирменный приказ, архивная запись и др.

Индикация подлинности любой реализации оригинала с течением времени становится технически сложной задачей. Существование оригинала может подтвердить только документ-копия, выданный уполномоченным на то хранителем архива документов, гарантирующим соответствие ее содержания документу-оригиналу, занесенному в архив много лет назад с ЭЦП, утратившей в данный момент свою актуальность. Естественно, что документ-копия заверяется действующей в момент выдачи ЭЦП хранителя архива.

Вторая причина — физическое старение документа, подразумевая под этим утрату им после применения возможности быть формальным основанием прав и обязанностей участников информационного взаимодействия. Такое характерно, как правило, для документов кратного действия, например, платежного поручения. Подобный документ после его применения должен тем или иным образом «погашаться», терять юридическую силу. В аналоговой среде пометка о погашении ставится на оригинале, документ сохраняет «похожесть», так что это допустимо. В электронном документе присоединение пометки о погашении при соблюдении условия ее неотделимости от исходного документа-оригинала ведет к другому, с позиций правил среды, документу, который и должен рассматриваться как документ-копия, подтверждающий существование оригинала в каком-то из прошедших моментов.

Электронный документ-копия (ЭлД-копия) — электронный документ, содержание которого тождественно ЭлД-оригиналу, но атрибуты ЭлД-копии отличаются от атрибутов ЭлД-оригинала.

Обратим внимание на тождественность содержания документа и документа-копии. Это обусловлено цифровой природой сектора действенности ЭлД. В аналоговом мире достаточно одинаковости (не обязательно тождественности) содержания. Более широкий пробел между словами в аналоговом тексте не сказывается на одинаковости, но для

цифрового документа лишний пробел означает два разных документа. Если «копия» ЭлД изоморфна оригиналу, то это не «копия», а «тот же самый документ». Если нет — то «совершенно другой», и, значит, не копия.

Можно и нужно говорить о двух *разных* электронных документах, называя их, например, «ЭлД-оригинал» и «ЭлД-копия», понимая под этим изоморфизм не полных множеств (целиком), отображающих документы, а некоторых подмножеств (части) этих множеств. Признак, указывающий объектам электронной среды, как выделить («вырезать») подмножество, должен быть задан заранее. Например, весь текст документа без цифровой подписи. Назначение ЭлД-копии — доказательство существования ЭлД-оригинала с таким же содержанием.

Строго говоря, и в аналоговой среде оригинал и копия — это разные документы, они предназначены для выполнения различных функциональных задач. Оригинал правового документа определяется как признаваемое сектором действенности *формальное основание для изменений правоотношений* между участниками информационного взаимодействия. Копия документа — это признаваемое сектором действенности *свидетельство существования оригинала* с таким же содержанием. Например, некоторое право обеспечивается Законом, подписанным Президентом, но не его официальной публикацией, ссылаются на Закон, но не на его публикацию. Публикация только подтверждает, что такой Закон действительно существует и подписан. Оригинал и копия предназначены для выполнения разных функций, значит, это разные документы.

Так как копия это другой документ, то и ее юридическая сила отлична, в общем случае, от оригинала. На одно из отличий, разное целевое назначение оригинала и копии, мы уже указали. В ряде ситуаций значимость достоверности копии может быть настолько велика, что

необходимо предъявление документа-копии более высокого ранга или исходного документа-оригинала. Под рангом копии здесь понимается репутация изготовителя документа-копии. Менее очевидно другое отличие — невозможность соблюдения требования кратности применения документа: существует *только один оригинал*, но может быть *несколько копий*. Это не исключает уникальности каждой копии, их атрибуты отличны, но нельзя «отследить» суммарное количество практического применения оригинала и всех его копий.

Смешение понятий оригинала и копии при аналоговом документообороте не ведет к заметным негативным последствиям в силу участия мыслящего субъекта, автоматически отслеживающего сомнительные случаи за счет неформального расширения множества подлинности. Но в электронном документообороте неформальные действия невозможны по определению. К тому же существенно возрастает возможность подделки документа: цифровое множество атрибутов, как уже установлено, потенциально много уже аналогового, а копирование и модификация электронного сообщения несравнимо проще аналогового.

В результате приходим к напрашивающемуся выводу, имеющему принципиальный характер для электронного документооборота. *В электронной среде не может существовать двух одинаковых документов, любой ЭлД, понимаемый как множество эквивалентных реализаций, уникален.* Если это оригинал, то вопросов не возникает, оригинал может быть один и только один, иначе машина не сможет проводить формальные преобразования. Если это ЭлД-копия, то должна обеспечиваться возможность сопоставления его содержания с ЭлД-оригиналом либо с документом-копией более высокого ранга.

2.3.5. Электронная среда как пространство чисел и функций (отображений)

Ранее было установлено качественное, системное отличие свойств электронной и традиционной, аналоговой, среды взаимодействия. В электронной среде теряют свою адекватность ряд распространенных терминов и понятий, закрепленных в массовом сознании многовековым опытом работы с традиционной формой отображения документа в виде текста на листе бумаги, понимаемых по умолчанию. Выделим поэтому ряд принципиальных положений, характерных для электронной формы отображения и преобразования информации. Исходя из предмета анализа, ограничимся только понятийным комментарием, более аккуратно это изложено в [12, 64].

Любой понятийный аппарат необходимо должен опираться на фиксированность описания, статичность исходных объектов и явлений, их инвариантность относительно точки пространства и/или времени, в которой эти объекты и явления рассматриваются. Для объекта или предмета требование соблюдается очевидным образом — аналоговый документ как предмет в любой момент и в любой точке остается таким же: лист бумаги, поверхность которого «раскрашена» линиями (буквами) другого цвета.

Статика характерна для аналоговой формы отображения информации и в электронной среде. Например, при хранении на диске памяти электронная информация отображается «раскраской» поверхности диска разной ориентацией магнитных доменов. Эта «раскраска» не меняется во времени и, значит, фиксирована. Обычно говорят, что в памяти ЭВМ хранятся данные, которые фиксированы в течение своего жизненного цикла. Данные понимаются как фиксированная форма существования информации.

В электронной среде теряет значимость свойство информации быть сведением, смыслом, знанием. Для компьютера стихи и случайное число в определенном смысле неразличимы — это множество двоичных бит, на

котором задан порядок — последовательность нулевых и единичных бит. Информация в электронной среде есть множество (сигналов), на котором задано отношение предшествования — отношение упорядоченности. Любые два множества отображают одну и ту же информацию, если сохраняется заданное отношение упорядоченности — если множества изоморфны. Любую двоичную ограниченную последовательность можно преобразовать в число, поэтому, слегка вульгаризируя, полагаем, что в электронной среде информация есть число. Число не меняется во времени и пространстве, оно всегда фиксировано. Учитывая сказанное выше, в дальнейшем полагаем, что информация — это число.

Компьютер — это не только память, но и вычисления. При изменении формата документа одни данные исчезают, другие возникают, а информация остается той же самой. Числа меняются, а информация — нет, так как сохраняется изоморфизм между множествами двоичных сигналов при «старом» и «новом» форматах. В аналоговой среде подобное почти невозможно: копия с АнД есть новый документ, исходный можно уничтожить или сохранить, но нельзя преобразовать. Таким образом, в электронной среде принципиально должна существовать некая новая форма существования информации, соответствующая процессу преобразования — информация не может исчезнуть между «входом» и «выходом» процесса. Эта форма имеет место в интервале времени между «старым» и «новым» форматами, если бы информация исчезала, то эквивалентность (изоморфность) форматов была бы невозможной.

Но в чем заключается фиксированность процессов или явлений, которые по определению динамичны, являются изменением чего-либо во времени? Если этого не выяснить, то понятийная база теряет устойчивость — нельзя «менять правила во время игры». Фиксированность процесса понимается как фиксированность его описания, в какой бы точке пространства (компьютере) и момент времени этот процесс ни

реализовался бы. Это возможно, например, конкретный процесс обработки информации в ЭВМ определяется фиксированным алгоритмом.

Допустив, что в электронной среде существуют две формы отображения информации: статическая — в форме объекта, динамическая — в форме процесса, мы тем самым допустили два класса элементов электронной среды. Коль скоро первый класс определен как числа, то второй класс логично назвать функциями. На «вход» функции поступают числа-данные, на «выходе» появляется новое число-данные. В любой момент времени и в любой точке пространства функция остается функцией. Функция или близкие понятия — отображение, алгоритм, преобразование — неизменны, фиксированы. При определенных ограничениях на свойства функции можно говорить о преобразовании информации.

В анализе понятие функции вводится следующим образом. Пусть X — некоторое множество на числовой прямой. На X определена функция f, если каждому числу $x \in X$ поставлено в соответствие определенное число $y = f(x)$. При этом X называется областью определения функции f, а Y — совокупность значений, принимаемых этой функцией — областью значений.

Определив информацию в электронной среде как упорядоченное множество, корректнее говорить о функции в обобщенном понимании — отображении множеств [67]. Если вместо числовых множеств рассматривать множества произвольной природы, то приходим к самому общему понятию функции. Пусть M и N — два произвольных множества. Говорят, что на M определена функция f, принимающая значения из N, если каждому элементу $x \in M$ поставлен в соответствие один и только один элемент y из N. Для множеств произвольной природы вместо термина «функция» часто пользуются термином «отображение», говоря об

отображении одного множества на другое. Для обозначения функции (отображения) из M в N будем пользоваться записью f: $M \to N$.

Если a — элемент из M, то отвечающий ему элемент b из N называется его образом (при отображении f). Совокупность всех тех элементов a из M, образом которых является данный элемент $b \in N$, называется прообразом (точнее, полным прообразом) элемента b и обозначается $f^{-1}(b)$.

Пусть A — некоторое множество из M; совокупность $\{f(a)$: $a \in$ A$\}$ всех элементов вида $f(a)$, где $a \in A$, называется образом А и обозначается f(А). В свою очередь для каждого множества B из N определяется его (полный!) прообраз f^{-1}(В), а именно — f^{-1}(В) есть совокупность всех тех элементов из M, образы которых принадлежат B. Может оказаться, что ни один элемент b из B не имеет прообраза, тогда прообраз $f^{-1}(B)$ есть пустое множество. Если $f(M) = N$, то f есть отображение множества M «**на**» множество N. Когда $f(M) \subset N$, то говорят, что f есть отображение M «**в**» N.

Понятие «отображение», по существу, есть обобщение «функции», но предполагает более широкий спектр возможных соответствий и практически неограниченно расширяет физическую природу сопоставляемых множеств.

При анализе информационного обмена в электронной среде целесообразно базироваться на понятиях «число (данные)», «функция (процесс)».

2.4. Выводы

1. Традиционно понимаемый (аналоговый) документ существует и действует в среде, образованной мыслящими субъектами, аналоговой среде. Электронный документ — в электронной (цифровой) среде,

образованной неодушевленными, цифровыми программно-техническими объектами. Аналоговый документ размещен в пространстве, активизированный электронный документ размещен во времени. Аналоговый документ не воспринимается объектами электронной среды, электронный документ не воспринимается субъектами (людьми) аналоговой среды. В аналоговой среде множество, моделирующее документ, имеет бесконечную мощность и является непрерывным, в электронной — конечную мощность и является дискретным.

Отличие аналоговой среды от электронной, традиционного документа — от электронного, имеет качественный, системный характер.

2. Аналоговая среда — среда неоднозначности и приблизительности, электронная — однозначности и точности. В аналоговой среде восприятие информации одномоментно, целостно, в электронной среде восприятие информации последовательно и фрагментарно. Аналоговый документ статичен и может быть зафиксирован, электронный документ — это динамичный объект, не может быть зафиксирован, и в активизированном состоянии должен рассматриваться как процесс.

3. Любой документ состоит из двух компонентов: один из них, «содержание», реализует прямое, информационное назначение документа; другой, «атрибуты» — вспомогательные функции, обеспечивает необходимые условия для восприятия и обработки документа и придает содержащейся информации статус документированной. Информация всегда конечна и может быть отображена конечным множеством элементов. Атрибуты аналогового документа отображаются множеством бесконечной мощности, атрибуты электронного документа — множеством конечной мощности.

4. Избыточность электронного отображения информации в силу конечности множества, отображающего ЭлД, много ниже, чем в случае АнД. Но избыточность и есть тот ресурс, который используется для

обеспечения вспомогательных функций документа: обеспечения помехоустойчивости, защиты информации, придания документу юридической силы и др. Проблемы защиты, обеспечения правомочности электронных документов должны решаться принципиально много сложнее, чем аналоговых.

5. Электронный документ нельзя рассматривать в отрыве от (фрагмента) электронной среды. Защита ЭлД необходимо должна включать и защиту его преобразований — факторов, инвариантных относительно ЭлД, не зависящих от него.

Электронный документ определяется как пара: сектор действенности и сообщение, оформленное в соответствии с правилами сектора действенности. В рамках сектора действенности документ признается фактом — формальным основанием для возникновения, изменения, прекращения конкретных процессов преобразования документа элементами электронной среды, принадлежащих сектору.

6. Информация в электронной среде есть маркированное известным способом конечное дискретное (цифровое) множество элементов, на котором задано бинарное отношение упорядоченности: для любой пары элементов известно предшествование одного другому. Основным требованием к преобразованию информации в электронной среде является сохранение отношения упорядоченности — (вычислимый) изоморфизм отображения множества, маркированного как «информация».

7. Электронный документ есть множество неразличимых эквивалентных реализаций, любая из которых полностью характеризует множество. Идентификация множества, т. е. собственно ЭлД, возможна на основе любого подмножества, вплоть до одной реализации. Любые два изоморфных множества элементов (сигналов), содержащих одну и ту же информацию, эквивалентны по критерию упорядоченности элементов, логически неразличимы, могут быть преобразованы одно в другое,

отображают одну и ту же информацию.

8. В любой момент времени существует один и только один ЭлД (понимаемый как множество реализаций!) с данными параметрами — любой электронный документ уникален. Электронный документ-оригинал и электронный документ-копия есть два разных документа, имеющих разные атрибуты, но эквивалентные (изоморфные) содержания. Применительно к электронному документу не имеют содержательного смысла понятия «идентичные ЭлД», «одинаковые ЭлД», «экземпляры ЭлД». Назначение документа-оригинала — служить формальным основанием для изменений правоотношений между участниками информационного взаимодействия. Назначение документа-копии — служить доказательством существования оригинала с таким же содержанием.

9. Оформление документа обеспечивается совокупностью его атрибутов, в достаточно широких пределах не зависящих от содержания документа, постоянных для каждого класса документов. Атрибуты должны, в общем случае, предусматривать реализацию в рамках сектора действенности:

- индикации целостности документа;
- доступности содержания документа объектам сектора действенности;
- недоступности содержания документа объектам иных, априорно заданных, секторов действенности (конфиденциальность);
- аутентификации автора и/или отправителя документа;
- аутентификации получателя и/или адресата документа;
- аутентификации маршрута (промежуточных точек) прохождения документа от отправителя до получателя;
- кратности прикладного использования документа.

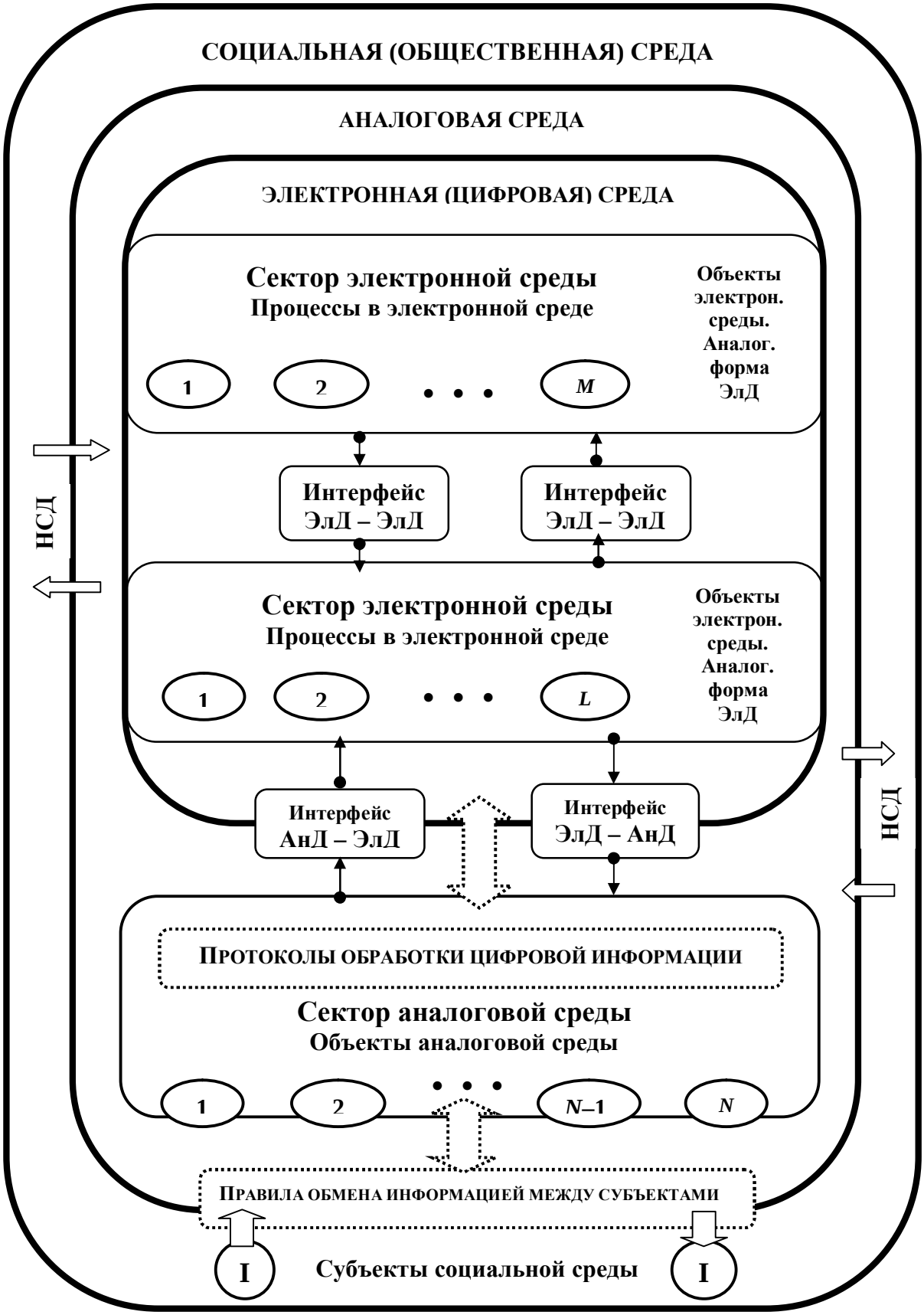


Рис. 3.1. Три среды существования документа — социальная, аналоговая, электронная

Глава 3. **ОСНОВЫ ПОНИМАНИЯ ФЕНОМЕНА ЭЛЕКТРОННОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ**

Когда древние считали, что Земля плоская, это не мешало их жизнедеятельности. И только при переходе к длительным путешествиям, самолетам и ракетам, ошибочность предубеждения оказалась значимой.

В течение многих веков удаленное информационное взаимодействие осуществлялось на основе традиционных технологий изготовления документа — раскраской цветными узорами (буквами и картинками) поверхности предмета (листа бумаги). И определение документа как «…зафиксированной на материальном носителе информации с реквизитами, позволяющими ее идентифицировать» [23, 30] было полезным. Но сейчас, с появлением электронного документа, применяемого на основе новых информационных технологий, подобная трактовка становится неконструктивной. В Федеральном законе [26] от 10.01.02 г. понятие ЭлД определяется как «… *документ, в котором информация представлена в электронно-цифровой форме*». Является ли изображение документа на экране монитора цифровым документом? Попробуете найти электронную форму на перфокарте?

Неверно определять документ только внешними признаками его технологической реализации, внешние признаки обманчивы — сегодня брюнетка, а завтра блондинка. Необходимо сначала разобраться в исходном понятии — что же такое феномен электронного удаленного взаимодействия? — и только потом попытаться понять, чем же отличается одна из технологических форм реализации документа — электронная, от другой — аналоговой. Во главе угла должны быть функции, задачи того материального явления, которое выбрано обществом в качестве документа.

Документ как изделие — всего лишь посредник (агент) информационного взаимодействия. Для окружающего нас мира базовыми являются две материальные категории существования — материя и энергия. Не вдаваясь в тонкости трактовки этих категорий, можно

отождествлять материю с «предметом, объектом», а энергию с «сигналом, процессом». Предмет (материя) как носитель документа традиционен и не вызывает недоумения, тогда почему отказывать в возможности такого применения процессу (сигналу, энергии). Возможны два кардинально отличных вида изделий-носителей сообщения (документа): предмет-«материя» и процесс-«энергия». Установлены родство изделия-предмета с таким понятием как «пространство», а изделия-процесса — с таким как «время».

Основным преимуществом предмета в качестве носителя документа является неизменность его параметров в течение длительного времени. Это свойство отвечает требованию *транспортировки во времени — хранения* документа. В активизированном состоянии (в режимах передачи, обработки) сообщение существует в форме процесса (сигнал, энергии). Из физических законов следует, что таким образом решается проблема *транспортировки информации в пространстве*. Оптимальным решением из экономических соображений является тот случай, когда технология предусматривает при передаче форму сообщения в виде сигнала, а во время хранения — предмета. Это новые информационные технологии — НИТ.

3.1. Документ как материальный посредник информационного обмена

3.1.1. Три среды существования документа (сообщения) — социальная, аналоговая, электронная. Документ как информационный факт

Среди множества понятий, отражающих разные стороны документа, безразлично — электронного или традиционного, нам наиболее подходит определение Федерального закона «Об обязательном экземпляре документов» [24]: «*документ — материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях*

хранения и общественного использования». Определение принято еще в эру безграничного господства документа на традиционном (бумажном) носителе, поэтому не будем обращать внимание на слова «материальный объект». Электронный документ может быть и в форме «материального процесса», при этом нужен специальный комментарий, чтобы представить себе «зафиксированный процесс». Конечно, «… предназначенный для передачи во времени и пространстве в целях хранения …» — это промежуточная, подчиненная цель — не все ли равно, как документ будет транспортироваться, передаваться и/или храниться, лишь он был бы предъявлен «в нужном месте и в нужное время». Для нас важно, что основной функциональной целью документа является *общественное* использование.

Жизненный цикл сообщения, документа протекает в трех средах существования (Рис. 3.1). Внешняя образована социальной средой, подмножество мыслящих субъектов которой формирует сектор действенности документа. Общество, но не отдельный субъект, диктует правила обмена информацией своим членам-субъектам. Выполнение продиктованных социумом требований в документе или сообщении обеспечивает возможность однозначного толкования его содержания элементами сектора действенности. При ошибочной трактовке сектором действенности наказывается, по крайней мере, либо автор, либо пользователь.

Остальные две среды имеют дело не со «знанием» и «сведениями», но с *материальным* отображением информации: аналоговой — в виде предмета; активной электронной — в виде процесса. Машина не умеет мыслить, она умеет только преобразовывать выделенное тем или иным способом множество сигналов на основе однозначно заданной последовательности фиксированных операций. Говоря об информационном обмене, мы обязаны, в первую очередь, исходить из требования эффективности терминологии применительно к описанию

среды, формируемой неодушевленными объектами. Почта, архив, телефон, телефакс, компьютер и т. д. — все это такие объекты. Вербальное описание аналоговой и электронной среды было дано в предыдущем главе.

Простой пример: на заседании суда экран только что был белым, но вот включили проектор — и на экране появился видеофильм. Является ли изображение документом, если его нельзя даже «потрогать»? Если не является, то решение суда, вынесенное на основе просмотра, будет обосновываться не документом, а чем-то посторонним. В то же время, предъявление членам суда в качестве документа видеокассеты означает всего лишь показ пластиковой магнитной ленты коричневого цвета, на ней ничего разглядеть нельзя, да и на кинопленке отдельные кадры не дают представления о динамике развития события. Утверждаете, что изображение не документ, но его копия? Но, во-первых, копия это также документ, хотя и с меньшей степенью доказательности, и мы опять возвращаемся к предыдущему. А во-вторых, зачем же принимать решение на основании копии, когда оригинал лежит в паре шагов от экрана.

Если же согласиться, что на экране представлен документ, то придется признать и ряд вытекающих отсюда следствий. Например, что на ряде этапов жизненного цикла документ может не являться предметом, а может являться процессом, что может существовать одновременно в различных точках пространства — на экране и на видеокассете; что документ не всегда является только «…зафиксированной на материальном носителе информацией»; что вопреки определению оригинал не единственен. Можно выдвинуть в поддержку старого определения целый ряд уточнений, но ведь и пример приведен традиционного документа, не электронного.

Его задача — быть «звонком», иллюстрировать, что уж если традиционное толкование вызывает такие вопросы даже при рассмотрении аналогового документа, то не исключено, что при анализе на старой базе

электронного документа уточнений найти не удастся. Вот, например, передача по радиоканалу: ЭлД нигде не зафиксирован; в любом месте радиоприема доступен; единственный оригинал исходного сообщения превращается там, где стоят приемники, во множество неразличимых реализаций. В общем, ни одному из «старых» определений электронный документ не удовлетворяет, так что его передача с юридической точки зрения невозможна.

Документ есть явление социальное, присущее только общественной жизни мыслящих субъектов: в мире животных документа нет и быть не может, хотя обмен информацией имеется. Назначение документа — признаваемое обществом, т. е. *легитимное* (от лат. legitimus — согласный с законами, правомерный), объективно существующее формальное информационное основание для тех или иных действий участников информационного обмена.

В правовой сфере есть понятие [7] *юридический факт — предусмотренные в законе обстоятельства, при которых сохраняются или изменяются (возникают, прекращаются) конкретные правоотношения между участниками взаимодействия.* Признание документа сообщением о юридическом факте в социальной среде — не произвол участников обмена, такое обеспечивается силой — обществом в лице государства. Эта высшая относительно любого из участников инстанция, используя свои институты поощрения и наказания, предопределяет однозначную интерпретацию содержания, диктует реакцию участников на документ, предоставляет им права и налагает обязанности. Попробуйте неправильно понять и применить «Правила безопасности дорожного движения», и штраф неизбежен.

Однако юридический факт в рамках одного государства не является таковым в другом: российская банкнота как документ предоставляет право его обмена на товар только в России, но не в Зимбабве. Тем самым, говоря о документе, явно или неявно задается часть мирового общества, в данном

случае — государство, в пределах которого он признается юридическим фактом. Тогда почему не считать, что некий объект или явление, не предусмотренные в явном виде в государственных законах, являются, тем не менее, достаточным основанием для сохранения и/или изменения взаимоотношений в рамках *части* общества страны.

Роль законов в таком фрагменте общества, члены которого объединены общими профессиональными, деловыми, или родственными интересами, играют неформальные, явные и неявные правила и обычаи, выработанные и «принятые к исполнению» *всеми* его членами. Здесь документ информирует уже о не *юридическом*, но просто о *факте*. Этот фрагмент общества (группу) будем называть *сектором действенности* документа. Как и в случае с государством, интерпретация документа, правила поведения каждого члена сектора диктуются *извне*, также действуют институты поощрения и наказания, они, быть может, не столь категоричны как государственные, но порой более эффективны.

Записка директора является для работника документом в рамках фирмы, неисполнение указания влечет наказание, хотя бы падение деловой репутации работника. Чертежи машины являются на заводе документом, нестыковка размеров влечет штраф для исполнителей. Точно также частное письмо, например, с просьбой выслать денег, является документом в среде, образованной корреспондентами и их родственниками, друзьями, знакомыми. Верно и обратное: сектор действенности — это такой фрагмент общества, в котором документ признается сообщением о факте. Частное письмо между знакомыми мужчиной и женщиной есть факт не только для самих корреспондентов, но и для их близких родственников: для первых — позитивный, для вторых — негативный, они инициируют разные изменения отношений, но это факты.

Так как любой сектор действенности документа есть часть общества, то можно построить **иерархию** секторов, например, мир, государство, отрасль, фирма, знакомые, семья. Требования, которые сектор

действенности предъявляет для придания сообщению статуса документа, могут вырабатываться и на высших уровнях иерархии, но, все равно, они должны быть «ратифицированы» сектором. Язык, семантика, синтаксис, грамматика и оформление частного письма в главной своей части диктуются обществом, а не взаимодействующими корреспондентами и их ближайшим окружением. Но сектор ретранслирует и/или модифицирует эти требования применительно к устоявшимся среди своих членов нормам, правилам и обычаям информационного взаимодействия. Обращение «Дорогой Вова!» вряд ли характерно для служебного письма, но оно применимо к частному сектору действенности, образованному кругом знакомых.

Развивая иерархию, приходим к тому, что прямыми участниками электронного взаимодействия являются сектора из неодушевленных объектов. Правами и обязанностями эти объекты обладать не могут, но можно говорить о возможностях и ограничениях, накладываемых сектором действенности на свои компоненты. В электронном секторе правила (алгоритмы) трактовки ЭлД детерминированы, определяются обязательно вне рамок сектора, но точно также доводятся «до сведения» его членов, программно-технических объектов. Как и в социальной среде, эти возможности и ограничения относительно объектов сектора действенности ЭлД определяются «внешней силой». Но здесь эту роль играет субъект, ретранслирующий правила, установленные (техническом) обществом, и определяющий состав и конфигурацию инструментальных средств, программно-техническую базу, правила доступа, алгоритмы и дисциплину обработки, передачи и хранения ЭлД в системе.

Не уменьшая общности можно полагать, что *все* требования к документу формируются «напрямую» его сектором действенности. Таким образом, корректное задание документа означает определение **пары: {**сообщение, закрепляющее факт; сектор действенности}.

Документ является сообщением о факте, которое признается в рамках сектора действенности легитимным основанием для сохранения, изменения, прекращения определенных взаимоотношений между членами сектора.

3.1.2. Функциональное назначение документа — его демонстрация

Необходимым и достаточным условием для того, чтобы документ выполнял роль информационного факта, является его демонстрация по требованию сектора в заранее неопределенных моментах времени и точках пространства. При таком условии остаются в стороне требования к документу [24] «…предназначенный для передачи во времени и пространстве в целях хранения …». Это, с позиций математики, абсолютно лишнее ограничение. Не все ли равно, как документ добирается до точки демонстрации, а может, например, документ изготовлен из полуфабрикатов непосредственно в этой точке. Вам никогда не приходилось ездить в учреждение с пустым бланком письма, на котором есть только исходящий номер, печать и подпись руководителя, чтобы заполнить его там задним числом?

Чтобы обеспечить демонстрацию, документ должен быть реализован в материальной форме и предъявлен социуму в виде изделия. Система **чисел**-параметров данного изделия, считанная в определенном **порядке**, вполне «пригодна» для отображения информации, носителем которой это изделие является. Это вполне отвечает отображению в виде упорядоченной совокупности также нематериальных чисел — результатов физического измерения параметров изделия. Здесь мы сталкиваемся с понятием *порядка* для «информации». Документ как изделие функционально служит лишь отправной точкой для различения порядка параметров.

Демонстрация документа — это предъявление в нужном месте и в нужный момент изделия-носителя информационного факта для того,

чтобы с него были сняты ***предложенным сектором действенности*** *способом параметры изделия — характеристики информации.*

Необходимо разделить два аспекта документа:

- нематериальный — правовой, признанное сектором действенности (группой) общества формальное основание определенных взаимоотношений;
- материальный — технологический, закрепленное созданным человеком способом отображение информации в виде изделия, которое может быть продемонстрировано группе как некоторый предмет или процесс.

Выделяются два класса требований — семантические и технологические.

Семантические требования относятся к смыслу, сущности информации, являющейся содержанием («текстом») документа, а также идентифицирующей авторов и/или пользователей документа. Их соблюдение — обязанность субъекта-автора, формирующего текст документа и выбирающего признаки легитимности документа в секторе действенности. Выполнение семантических требований, тесно связанных с процессом мышления человека, продиктованных социумом, обеспечивает возможность однозначного, с позиций сектора, толкования содержания документа элементами сектора. При ошибочной трактовке наказывается сектором действенности либо автор (если документ нечеткий, или если сообщение нелегитимно), либо пользователь (если документ неправильно «понят»). Семантические требования лежат вне темы данной работы, рассматривающей документ как материальный посредник информационного взаимодействия.

Технологические требования точно также задаются социальным сектором действенности документа, который *предписывает*, чтобы способ *материального* представления (отображения) информации необходимо обладал рядом специальных, заданных сектором, характеристик. Правила

дорожного движения должен соблюдать не автомобиль, а водитель, но автомобиль как изделие должен обладать свойствами управляемости, торможения, регулирования скорости и др.

Действия сектора действенности маскируются субъектом-хозяином технологических средств, но, в главном, он следует рекомендации сектора. Например, он не может перейти к десятичной системе счисления, хотя ее отличия от двоичной, с позиций математики, нет. По существу, налагаются ограничения на процессы отображения информации в течение всего жизненного цикла документа: изготовления, обработки, передачи и хранения документа. Только тогда прямые участники (автор, адресат и др.) могут использовать документ как формальное основание правоотношений как между собой, так и с третьими лицами (субъектами социальной среды), а посредники приобретают право на оплату услуг за реализацию информационных технологий.

3.1.3. Содержание и атрибуты — переменная и постоянная части документа

Для того чтобы демонстрация изделия выполняла функцию факта, необходимо требуется, чтобы *содержание* документа было постоянным, равнялось бы содержанию в момент создания. Содержание документа, в принципе, случайное событие, иначе, зачем документ нужен. Остается только одно — некоторые параметры, непосредственно связанные с отображением информации (содержанием) демонстрируемого изделия, должны быть неслучайны, «знакомы» членам сектора действенности. Таким образом, неслучайным может быть только оформление — атрибуты документа и технология преобразования, передачи и хранения документа. Обобщается понятие документа: «…информация с *реквизитами*, позволяющими ее идентифицировать»; согласно ГОСТу [30], «реквизит документа — обязательный элемент оформления официального документа».

Возникает вопрос: «получаемый документ заранее неизвестен, так можно ли знать его параметры (эталонные параметры, параметры эталона) в прошлом, в точке формирования?» Вопрос естественен, так как понятие «документ» прочно ассоциируется с семантическими особенностями, с его содержанием, информацией. Но ведь здесь рассматривается документ как технологическое изделие. Кроме того, не предполагается, что должны быть известны **все** характеристики исходного документа! Сектор действенности, предписывая технологию изготовления документа, задает ряд параметров, значения которых для демонстрируемого документа являются необходимым условием отсутствия искажений содержания.

Изделие-документ обязательно должно характеризоваться двумя группами параметров: основные, условно-переменные — отражающие содержание; вспомогательные, условно-постоянные. Последнюю группу параметров будем называть атрибутами документа, включая в их состав и реквизиты документа как частный случай априорно заданных констант реализации документа в виде предмета или процесса. Выходит, что в состав документа-изделия непременно входит ряд эталонных (условно-постоянных) параметров. Только тогда, когда в выполнении этого требования сектор действенности *убежден*, возникают достаточные основания для признания сектором информации документированной, а сообщения — *документом* с закрепленной в нем информацией о (юридическом) факте.

Демонстрация информационного факта предполагает, что заданные сектором действенности физически измеримые параметры изделия ***совпадают с параметрами эталона****, существовавшего в исходной точке.*

Для денежной банкноты известны размеры, размещение надписей, раскраска поверхности, прочность связи краски с носителем, физические характеристики бумаги, даже содержание имеет очень ограниченное число вариантов. Не говоря уже о более слабых признаках: источник документа,

трасса прохождения, контекст содержания и др. И для содержания, условно-переменных параметров документа, исходя из того, что любое измерение параметра — это число, можно сконструировать ряд количественных инвариантов: например, хэш-код, электронную цифровую подпись. Значит, можно предписать, чтобы значения числа-содержания в точке формирования документа удовлетворяли бы неким заранее заданным параметрическим уравнениям.

3.1.4. Свойства документа — доступность, целостность, легитимность

Документ как изделие — это средство (агент, материальный посредник) взаимодействия членов (элементов) сектора действенности. На протяжении жизненного цикла, по инициативе одного или нескольких членов сектора, документ должен быть продемонстрирован другим членам сектора — предъявлен в произвольном месте в течение конечного времени с момента инициативы. В точке демонстрации необходимо:

- измерить эталонные параметры предписанными сектором действенности средствами измерения;
- если отличие *всех* измеренных параметров от эталонных лежит в пределах, разрешенных сектором, присвоить изделию статус документа;
- в противном случае забраковать изделие.

Отсюда вытекают базисные требования к материальной реализации документа: доступность, целостность, легитимность.

Доступность *— физическая возможность измерения заданных параметров изделия-документа (содержания, атрибутов, технологии) предписанными сектором действенности средствами в заданных точках «пространство-время» в течение конечного времени с момента возникновения потребности в демонстрации.*

Измерение есть объективная процедура, и это значит, что измерительные технологии и приборы должны с высокой достоверностью обладать требуемыми сектором действенности качествами, и, как

следствие — должны предписываться сектором. Ведь статус документа присваивается сектором, а не отдельным его членом. Так как технология измерения параметров задается сектором действенности, то время собственно измерения известно достаточно точно, и лимитирующим фактором является время доставки, перемещения документа к месту и моменту демонстрации. Передача и хранение документа есть вспомогательные процедуры: не имеет значения, где и как хранится или передается документ, важна только возможность его демонстрации за конечное допустимое время с момента возникновения требования.

Целостность *— при любой демонстрации изделия-документа* ***эталонные*** *значения заданных сектором физических параметров демонстрируемого документа-изделия должны лежать в заданном допуске соответствующих параметров атрибутов документа в начальной точке жизненного цикла.*

Часто целостность трактуется как отсутствие искажений или изменений в документа в течение его жизненного цикла. Это не точно. При трактовке документа как факта необходимо определить, что считается его искажением. Например, является ли искажением документа изменение его размеров при демонстрации на экране? Или изменение формата хранения ЭлД? Или распечатка электронного документа — здесь заменяется носитель документа? Определение не должно базироваться на «отсутствии искажений» характеристик содержания — таких может быть бесконечно много, а должно опираться на «*наличие постоянства*» некоторых из них. Во-первых, установить наличие чего-нибудь проще, чем отсутствие; во-вторых, количество имеющихся признаков много меньше, чем отсутствующих.

Сектор действенности устанавливает, какие именно параметры документа-изделия должны быть постоянными, остальные можно не измерять. Требование постоянства документа в течение жизненного цикла явно завышено — документ индицируется как факт только при

демонстрациях, суммарное время которых несопоставимо меньше жизненного цикла.

Легитимность *(лат. legitimus — законный, правомерный) — демонстрируемый изделие-документ должен содержать параметры, объективно подтверждающие правомерность использованных на протяжении жизненного цикла документа технологий.*

Легитимность — независимое базисное требование, не вытекающее из требований доступности и целостности, характеризующих собственно документ. Критерии легитимности выполняют вспомогательные функции, описывают *среду* формирования и существования документа между демонстрациями, что далеко не одно и то же. Легитимность означает, что документ содержит ряд параметров, значения которых так или иначе подтверждают, что использованные до момента демонстрации технологии формирования, обработки, передачи, хранения документа соответствовали требованиям, необходимым для признания изделия-документа фактом. Приведем несколько примеров.

Закон как документ должен содержать объективные доказательства официальной публикации, поэтому разрозненные страницы, содержащие текст закона, не являются документом, даже если они вырваны, например, из «Собрания законодательства РФ». Текст доступен, целостен — но не легитимен. Демонстрируемый на экране видеофильм доступен и целостен, если имеются достаточные гарантии, что он не подвергался монтажу, и не использовались спецэффекты. Но статус документа видеофильм приобретет только тогда, когда есть уверенность, что проецирующая аппаратура не подменяет изображение. Секретная почта, доставленная посторонним прохожим, а не фельдсвязью, вряд ли получит статус документа.

Или, например, аутентификация документа — объективное подтверждение приведенной в нем информации, идентифицирующей, например, автора или адресата документа. И субъекты аутентификации, и

документ существуют независимо друг от друга, физически разделены. А сектору нужны гарантии, что именно этот документ (изделие) сформирован (изготовлен) именно этим автором или получен именно данным адресатом. В качестве доказательства сектор предписывает, например, подписать документ и поставить печать, причем образец подписи и печати предварительно зарегистрировать в третьем месте.

Сигнатура, называемая подписью, и рисунок, именуемый печатью, никоим образом не влияющие на содержание документа, должны быть, тем не менее, еще и зарегистрированы в третьем месте. Для электронного документа те же самые функции выполняет абсолютно случайное число, называемое ключом цифровой подписи. Ясно, что регистрация есть составная часть технологии изготовления, хотя и не имеет непосредственного отношения к данному документу.

Напомним – документ – это пара **{**сообщение, закрепляющее факт; сектор действенности}. Следовательно, требование к сообщению необходимо должно дополняться требованием к сектору. В данном случае, дополнительные требования выглядят следующим образом:

- **доступность** (параметров сообщения) – **конфиденциальность** (для подмножества субъектов сектора);
- **целостность** (параметров сообщения) – **инвариантность** (других параметров с точки зрения сектора);
- **легитимность** (применяемых технологий) – **вариабельность** (других технологий с точки зрения сектора).

Как пример, рассмотрим дополнительное требование конфиденциальности. Сектор действенности требует, чтобы определенные параметры документа (текст) не могли бы наблюдаться заданным кругом субъектов или объектов (например, конкурентами), были бы им недоступны. Но это элементы того же самого сектора действенности, в котором документ должен быть доступен согласно первому базисному

требованию. Значит, должно быть определено ограничение, относящееся не непосредственно к документу, а к субъектам сектора, существующим вне зависимости от документа. Например, технология демонстрации предполагает дифференциацию субъектов сектора по допуску. Или только выделенная группа субъектов обладает средствами индикации (измерения) «смысла» документа — алгоритмами (ключами) шифрования и расшифрования.

3.2. Пространство и время, материя и энергия, предмет и процесс — формы существования отображения информации

3.2.1. Отображение информации — множество чисел-параметров изделия

Доминирующая трактовка понятия «информация», рассмотренная в главе 1 [1, 14—31], не соответствует перспективе массового применения документов в безлюдных технологиях. Собственно информация нематериальна, подобно таким нематериальным явлениям, как слово, идея, мысль, право, чувство. Это вполне отвечает ее отображению в виде упорядоченной совокупности виртуальных чисел. Отображение информации должно быть предъявлено в материальном виде изделия — предмета или процесса. Само по себе изделие необходимо должно быть феноменом материального мира. Таким образом, оно характеризуется объективно существующей системой физических измерений параметров изделия. Основу материальной реализации изделия, будь то в форме материи или в форме энергии, называют носителем информации или носителем документа. Только тогда можно применять количественные оценки, только тогда можно говорить о закрепленной информации, которая воспринимается неодушевленными объектами, инструментальными средствами вычислительной техники.

Существуют два способа измерений: аналоговые — отличием от эталона; количественные — числом эталонных единиц. Длину стержня

можно измерить линейкой, а можно просто сопоставить с двумя заранее изготовленными шаблонами, один из которых имеет максимально допустимую длину, другой — минимально. Для отображения информации в виде *предмета* — печатного текста на листе бумаги, поверхность которого «раскрашена узорами-буквами», существенно начертание букв и другие топологические характеристики его размещения на плоскости. Это измеримые параметры, другое дело, что проще измерить эти параметры шаблоном — закрепленным в сознании образом аналогового восприятия информации.

Отображение информации на листе бумаги задается изменением в пространстве цвета поверхности, положение каждой черной точки или линии зафиксировано в пространственной системе координат, жестко связанных с листом бумаги. Информация задается индикацией изменения цвета точек путем сканирования по пространству. На множестве поверхности листа определено отношение предшествования или упорядоченности различных точек (букв): обычно слева направо и сверху вниз, но может быть и более сложная топология, например, цветная картинка. Здесь мы сталкиваемся с понятием порядка для «отображения информации», само изделие функционально служит отправной точкой для различения *порядка* параметров.

Но вот характеристики документа в виде перфоленты или записи на дискете эффективнее измерять количественно. Здесь информация отображается двоичным числом конечной длины — такое сообщение называется цифровым. Вычислительная среда характеризуется обработкой и преобразованием информации на основе логических правил. Любой логический вывод есть совокупность последовательно выполняемых логических операций, поэтому множество, отображающее информацию, необходимо должно быть *последовательностью*. Не всякое множество есть последовательность, а только то, на котором задано отношение порядка.

Для ввода информации в вычислительную среду необходимо представить ее в виде *процесса* с фиксированной по времени очередностью характеристик. Активизированный электронный документ — это процесс (сигнал), электрические или электромагнитные характеристики которого изменяются во времени, их значения фиксированы во временной системе координат с началом отсчета, жестко связанного с началом активизации.

Отображение информации есть заданное сектором действенности и считанное в определенном ***порядке*** *множество (совокупность) физически измеримых параметров изделия-носителя: предмета, зафиксированного в пространстве; процесса, зафиксированного во времени.*

Отношение порядка на множестве должно быть «задано», а не «существовать». Должны быть известны признаки, позволяющие объектам электронной среды распознать это множество, для этого множество должно быть помечено, маркировано. Не требуется известность того субъекта или объекта, который задал отношение упорядоченности, важно только само отношение упорядоченности, которое должно «отслеживаться» программно-техническими объектами среды. Отображение информации — это маркированное детерминированным способом конечное множество, на котором задано бинарное отношение (частичной) упорядоченности: для любой пары элементов множества определено предшествование одного другому.

При информационном взаимодействии должно сохраняться отношение упорядоченности множества сигналов, маркированного как «информация», должен обеспечиваться (вычислимый) ***изоморфизм*** *преобразований.*

3.2.2. Математическая модель сообщения — пространство и время как категории отображения информации

И традиционное, и электронное сообщения используются для обеспечения взаимодействия субъектов экономики, так что их содержательное описание одинаково. Оба являются изделиями, пусть даже изготовленными по разным технологиям. Так ведь и традиционное сообщение может быть написано карандашом на листе промокашки, а может быть создано на основе последних технологических достижений. Очевидно, должна быть какая-то причина *системного* порядка для того, чтобы обусловить столь большую разницу в свойствах традиционного и электронного документа.

Из общей математической модели сообщения (документа) можно получить не совсем очевидные на практике следствия. Изделие-носитель D, находящееся в пространстве X и времени T, интерпретируется как некоторая многомерная функция $D(x, t)$, $x \hat{I} X$, $t \in T$, значений аргументов в окрестности $\chi \subset X$ точки пространства x и в интервале $\tau \subset T$ момента времени t. Формально аргументы x и t, χ и τ, X и T равноправны. Можно рассмотреть предельные случаи функции $D(x, t)$ и, если эти случаи «почти» совпадают с практическими феноменами, отождествить их с ними.

1. Изделие-носитель D сообщение от t не зависит. Отображение информации одинаково в любой момент времени, сосредоточено только в пространстве $\chi \subset X$ точки x, $D(x, t) = D(x)$, оно требует конечного объема χ пространства. Так как в состав аргументов время не входит, то интервал времени на съем информации лимитируется только средой существования изделия. В принципе достаточно «почти» нулевого времени, $\tau \approx O(0)$, восприятие информации одномоментное. Отображение считывается сканированием (порядок!) по пространству.

Примером такой пространственной категории является очень распространенный на практике носитель информации в форме предмета —

твердого объекта с устойчивыми во времени, но изменяющими в пространстве характеристиками, отображающими собственно информацию. К этому же классу параметров относятся: рельеф поверхности носителя — азбука Брайля для слепых; грампластинка, CD-диск; различная намагниченность пленки; прозрачность предмета — кинопленка и др. Для электронного документа в пассивном состоянии магнитный носитель есть та же самая страница с буквами, где «буквы» отображены «раскраской» поверхности диска магнитными доменами с разной ориентацией.

Отображение информации параметрами предмета характеризуется конечным объемом пространства и, если пренебречь старением носителя, то бесконечным временем существования.

2. Изделие-носитель D сообщение от x не зависит. Отображение информации присутствует во всех точках пространства X, но зато оно существует только во времени $\tau \subset T$ точки t, $D(x, t) = D(t)$. Объем пространства на съем информации лимитируется только воспринимающим объектом, иначе в состав аргументов сообщения неминуемо входило бы пространство. В принципе достаточно «почти» нулевого пространства, $\chi \approx O(0)$. Отображение считывается сканированием (порядок!) во времени.

К этому классу принадлежит категория носителя информации в форме процесса: сигнала с изменяющими во времени, но устойчивыми в пространстве физическими характеристиками, отображающими собственно информацию.

Например, сообщение правительства о дефолте, услышанное по радио. Документ? А как же, ведь имеют место «…предусмотренные в законе обстоятельства, при которых сохраняются или изменяются (возникают, прекращаются) конкретные правоотношения между участниками взаимодействия»: попробуйте получить деньги по валютному вкладу по прежней ставке. Отображение информации есть множество физически измеримых параметров процесса, считанных при помощи

шаблона — закрепленного в сознании образа речи. Всюду, где есть радиоприемник, этот документ не изменяется в пространстве *X*. На восприятие его нужно порядка минуты звучания, и никакие силы ни позволят сжать это время до секунд. На съем отображения информации, в принципе, требуется нулевой объем пространства: присоедините магнитофон к соответствующему контакту радиоприемника — объем (а не площадка!) контакта будет практически нулевой.

В приведенном примере все равно подразумевалось наличие носителя перед диктором радио, так что, хотя и с натяжкой, можно признать адекватным «… материальный объект с зафиксированной на нем информацией …». Но при переходе к электронному документу (ЭлД) и этот аргумент теряет силу, наглядный пример этого предельного случая — активная форма «электронного документа». Активный ЭлД существует только в процессе передачи, преобразования, в том числе записи и считывания, его носителем всегда является процесс, сигнал.

При оплате покупки в современном магазине кассир считывает штрих-код товара специальным приспособлением, преобразующим его в запрос в базу данных о цене. В ответ на ЭлД-запрос компьютер выдает ЭлД-ответ, поступающий в кассовый аппарат. Контроллер кассового аппарата на основе ЭлД-ответа формирует ЭлД-чек на покупку, который преобразуется в бумажный аналоговый документ (АнД), чек с указанием даты, стоимости, сдачи, времени и пр. Ни один из промежуточных ЭлД не зафиксирован на носителе, каждый существует *только* как процесс. Да, цена покупки, время, номер кассы, наименование магазина где-то хранятся в памяти, но это всего лишь отдельные компоненты, но не ЭлД в целом. Иначе и азбуку можно рассматривать как «зафиксированную информацию» любого текстового документа.

Активный ЭлД принципиально должен отображаться в последовательном виде, так что время передачи конечно, в то же время — сигнал индицируется на контакте, а объем контакта (пространство) можно

считать нулевым. Нуждается в объяснении, что такое «материальный процесс с зафиксированной информацией». ЭлД инвариантен к пространственным координатам, неточно локализован, сообщение одновременно присутствует в бесконечном числе точек пространства, либо не присутствует ни в одной точке.

3.2.3. Материя и энергия как категории носителей информации — физическая модель

Для окружающего нас мира только две материальные категории существования — *материя и энергия* — являются базовыми. С математической точки зрения это равноправные категории описания реального мира, в том смысле, что одна не является следствием другой, в математике говорят — базисные аргументы. Не вдаваясь в тонкости трактовки этих понятий, материя ассоциируется с «предметом, объектом», а энергия — с «сигналом, процессом». Предмет есть пространственная конструкция, тогда как сигнал — временная. Предмет как носитель документа традиционен и не вызывает недоумения: считанные в пространственном порядке измерения параметров отображают информацию.

Но тогда, гипотетически, такое же право рассматриваться как параметры отображения информации, имеют результаты физического измерения параметров энергии-процесса, считанные во временном порядке. И материя, и энергия материальны, измерение их параметров практически возможно — нет никаких оснований выбирать какую-то одну категорию в качестве приоритетной. Здесь возникает аналогия с предельными случаями: математическое описания сообщения $D(x, t)$: $D(x)$ — изделие-носитель расположено только в физическом пространстве X; $D(t)$ — сосредоточено только во временном пространстве T. Так математическая модель сообщения находит свое отражение в физической модели.

Это означает, что для отображения информации могут использоваться:

- пространственное изменение физических параметров *материи*, материального предмета, сосредоточенного в объеме *пространства* χ — традиционные технологии;
- временное изменение физических параметров *энергии*, материального сигнала, процесса, наблюдаемого в интервале *времени* τ — активные электронные технологии.

Аналоговое сообщение в форме предмета передается, хранится и демонстрируется в неизменной реализации. Столь очевидные процедуры передачи и хранения для традиционного сообщения в форме материи становятся непрозрачными применительно к отражению информации в форме энергии. Для хранения электронного сообщения применяется ориентация магнитных доменов на поверхности диска — аналоговая форма; для передачи используется последовательность электрических или электромагнитных сигналов — активная электронная форма; а демонстрироваться сообщение будет в третьей форме — смешанной. Интерфейсом преобразования «процесс (энергия) — предмет (материя)» служит, например, монитор. С «внутренней» стороны монитора — поток сигналов, а с «внешней» — аналоговое изображение на люминофоре экрана. Для электронного сообщения (документа) изделие-носитель не единственен в различные моменты времени и в разных точках пространства.

Хранение предмета требует в обычных условиях очень малой энергетики. Из общих соображений, для хранения (транспорт во времени) оптимально использовать отображение информации в виде предмета, так как сообщение $D(x)$ постоянно при любом t. Но высокоскоростная передача (транспорт в пространстве) документа в виде предмета неизбежно сопряжена с недопустимо высокими экономическими потерями — затратами на производство и поглощение энергии. Выход возможен

только на принципиально ином пути, передаче не самого предмета, а собственно информации.

Информация есть объект виртуальный, таким образом, ее отображение, по идее, малочувствительно к массе и размерам. Отображение информации, объект материальный, можно, таким образом, осуществить с почти нулевыми затратами. Если от передачи материальных частиц перейти к передаче свойств этих частиц в виде сигнала, то проблему энергетики в передаче отображения информации можно решить. Свойство индицируется только при воздействии на соответствующее устройство измерения, а воздействие есть сигнал, процесс. Сообщение $D(t)$ постоянно при любом x, для перемещения в пространстве (передачи) информации целесообразно применять ее отображение в виде процесса — энергии.

Если бросить камень в воду, то собственно частицы воды перемещаются очень незначительно по вертикали вверх — вниз, соответственно низка и энергетика, требуемая для их перемещения. В то же время само волновое возмущение (сигнал) распространяется по горизонтали на большое расстояние и с более высокой скоростью (волновая скорость). Точно также, вспышка на Солнце регистрируется через десяток секунд после возникновения, тогда как поток заряженных частиц, генерируемых вспышкой — через десяток суток. Сигнал перемещается много быстрее материальных частиц и требует несравненно меньших затрат энергии.

Человечество научилось усиливать энергетические явления, достаточно зафиксировать превышение весьма малого порога. Изменение сигнала индицируется на большом расстоянии в пространстве, можно сказать, что энергия (почти) инвариантна относительно пространства. Но тогда, обеспечив оперативную доставку документа в заданную точку пространства, сталкиваемся с проблемой обеспечения его демонстрации в течение произвольного времени. А это опять энергия — применение

сигнала для переноса информации целесообразно только в течение коротких фиксированных промежутков времени, много меньших жизненного цикла документа.

3.2.4. Перевод из процесса в предмет как основа демонстрации электронного документа

Сообщение всего лишь агент, информационный посредник, социального взаимодействия. Так как любой посредник не создает непосредственно материальных ценностей, то массовое применение находят только такие технологии посреднических услуг, которые экономят общественные затраты. Социальная функция сообщения (документа) обеспечивается в его демонстрации в отдельных точках континуума «пространство-время». Демонстрация — это предъявление изделия-носителя информации в нужном месте и в нужной момент для того, чтобы с него были сняты (измерены) предложенным сектором действенности способом параметры изделия — отражение информации.

Возможны два кардинально отличных вида изделий-носителей сообщения (документа) — предмет и процесс. Установлены взаимосвязи изделия-предмета с такими понятиями как «объект», «материя», «пространство», а изделия-процесса — как «сигнал», «энергия», «время». Из общих соображений следует, что предпочтительным местом поиска оптимального решения с позиций экономики является тот случай, когда технология предусматривает в передаче форму сообщения в виде сигнала, а во время хранения — предмета.

Быстрая передача документа в виде предмета неизбежно сопряжена с недопустимо высокими экономическими потерями. Хранение больших массивов традиционных документов, в виде пригодном для непосредственного использования, операция весьма дорогая, занимает, вдобавок к трудоемкости поиска, большой объем пространства – капитальных сооружений. Вместе с тем, «коэффициент полезного

действия» хранения близок к нулю — общество использует сообщения только во *время демонстрации*, занимающей пренебрежимо малую часть жизненного цикла, все остальное время документ «не нужен». Несмотря на указанные недостатки, традиционные технологии обеспечивают постоянное существование сообщения в виде неизменяемого предмета, что является *достаточным* условием выполнения требования передачи и хранения.

Возникает естественный вопрос, является ли такое условие одновременно и *необходимым*, другими словами, верно ли, что если документ не существует постоянно, то его невозможно предъявить для демонстрации? Не спешите давать утвердительный ответ. Пользователю безразлично, что демонстрируется, если выполнены требования сектора действенности по подлинности — равенству параметров (атрибутов, технологии) реализации и эталона. Коль скоро общество использует документ только эпизодически, то почему нельзя изготовить документ по требованию!

Время передачи должно быть конечным, поэтому документ не должен иметь огромное число «составляющих». Выход возможен только при передаче объекта «по частям», дезинтеграции на отображение информации на месте отправления и последующей их интеграции на месте приема. А это означает отказ от передачи характеристик материального носителя документа как предмета, их «слишком много». В то же время любое информационное сообщение всегда может быть отображено конечным числом параметров (знаков). Кардинальное отличие новых информационных технологий (НИТ) от традиционных заключается в том, что они базируются на изготовлении сообщения (документа).

Не совсем корректно утверждение, что на экране монитора компьютера воспроизводится записанный на диске документ. На диске записано информационное сырье — «полуфабрикаты», руководствуясь которыми из «расходного материала» — утилит прикладного ПО, на

«станках» — инструментальных средствах, создаются отдельные «детали» документа, которые затем «собираются» по «чертежам» — программным обеспечением, в готовое изделие – изображение на мониторе или распечатку на принтере. Аналогично, комплект технологической документации и комплектующие на изготовление автомобиля и сама машина — это разные объекты.

При отображении информации измерение параметра означает его преобразование в число, при сравнении двух конечных чисел можно однозначно утверждать, что эти числа либо равны другу, либо нет, третьего не дано. Двоичную ограниченную последовательность всегда можно преобразовать в число, т. е. в электронной среде информация есть число. Говорят, что в памяти ЭВМ хранятся данные, которые понимаются как фиксированная форма существования электронной информации — данные это число.

И действительно, изготовление сообщения есть синтез двух составляющих — сырья и станка. На «вход» процесса-функции поступает сырье — числа-данные, на «выходе» появляются новые изготовленные числа-данные. При преобразовании информации необходимо, чтобы динамичный процесс имел бы некую неизменную во времени фиксированную характеристику. И такая характеристика существует — это фиксированность описания процесса во времени, в какой бы точке пространства (компьютере) этот процесс ни наблюдался. Наиболее частое описание функции — это алгоритм, фиксирующий последовательность операций (преобразований) исходных данных.

Заметим, что изготовление свойственно только электронному документу. Находят свое объяснение и тенденции в практике защиты информации в электронной среде — расширение предметной области от защиты чисел — данных до защиты функций — вычислительной среды. Такое положение напоминает защиту карандаша, потому что им был или будет написан когда-то приказ. Это не нужно только потому, что в

традиционном документообороте часто отсутствует этап «изготовления». Но характеристики технологического процесса изготовления таких документов, как деньги — защищаются весьма тщательно.

При изготовлении исчезают все нюансы характеристик носителя аналогового документа в виде предмета, определяющих единственность, уникальность документа, его отличие от всех других «похожих». А как раз эти параметры позволяют индицировать искажение документа, гарантируют его подлинность, придают обычному информационному сообщению статус документа. Новые информационные технологии по самой своей сути не могут оперировать с интерпретацией оригинала как *единственного экземпляра* документа.

Да и понятие экземпляра электронного документа в традиционном понимании теряет содержательность. Ведь два экземпляра обычного документа содержат одинаковую информацию, но на различных носителях с длительным сроком жизни. Носитель активной электронной формы имеет очень малое время жизни: энергия рассеивается — носитель исчезает. Носитель аналоговой, пассивной формы обычно невозможно конкретизировать с точностью до отдельного документа — где-то в блоке памяти, либо носитель имеет временный характер — изображение на мониторе. Реализации ЭлД, представляя собой *один и тот же* документ, *обязательно* должны быть в каком-то смысле *неразличимы*, как две капли воды в стакане.

Подытожим теперь выводы насчет свойств новых информационных технологий (НИТ), проистекающих из развитых выше самых общих положений. Вызывает удивление, как много концептуальных свойств НИТ можно извлечь из такого общего, казалось, само собой напрашивавшегося материала.

1. Кардинальное отличие новых информационных технологий (НИТ) от традиционных заключается в том, что они базируются

на изготовлении сообщения (документа) в местах и моментах его демонстрации.

2. НИТ должны оперировать только с информационным (но не с материальным) аспектом сообщения или документа.
3. НИТ должны базироваться на процессе (энергии) как на носителе в части преобразования или передачи информации.
4. НИТ должны базироваться на предмете (материи) как на носителе в части хранения информации.
5. НИТ должны предусматривать преобразование динамичного энергетического процесса в статичные физические характеристики материального предмета, и наоборот.
6. НИТ должны предусматривать перевод сканирования по пространству в сканирование по времени, и наоборот.
7. НИТ должны оперировать только с множеством реализаций, представляющих собой одно и то же сообщение (документ).
8. Защита информации в среде НИТ должна включать и защиту чисел — данных, и защиту функций — вычислительной среды.

3.3. Правовые аспекты прикладного использования электронного документа

Среда существования ЭлД состоит из неодушевленных объектов, наказание и поощрение которых бессмысленно, а сам ЭлД не воспринимается человеком. Ситуация, на первый взгляд, парадоксальна, так как отношения между субъектами регулируются при помощи объектов (ЭлД), но субъекты не могут непосредственно воспринимать эти объекты. Разумеется, никакого парадокса нет, просто анализ правоотношений при электронном взаимодействии должен исходить из качественно отличной природы электронного документа.

Можно пойти по пути создания специализированного правового обеспечения электронного взаимодействия субъектов, выработки и

согласования многочисленных *новых* юридических норм и правил. Это процесс длительный, явно отстающий от наблюдаемых сейчас беспрецедентных темпов развития и применения электронного документооборота. Перспективным в таком случае является подход, опирающийся на отнесение (конечно, с соответствующими ограничениями) электронного документа к одной из известных юридических категорий. Это позволило бы использовать в сфере электронного взаимодействия тот огромный запас правовых норм, который наработан обществом применительно к подобным категориям.

3.3.1. Дуализм электронного документа — документ как информация и документ как вещь (предмет)

Определение документа в аналоговой среде: «идентифицируемая информация, закрепленная созданным человеком способом для ее обработки, передачи и хранения во времени и пространстве» — выделяет два главных аспекта документа. С одной стороны, документ есть информация, т. е. нечто нематериальное. С другой стороны, не просто информация, а «закрепленная» информация, что автоматически означает материальную реализацию. Уже здесь отслеживается двойственная природа, дуализм документа: документ как информация; документ как вещь, предмет — нечто, на чем эта информация «закреплена».

Вещь в праве — предмет внешнего (материального) мира, находящийся в естественном состоянии в природе или созданный трудом человека; основной объект имущественного правоотношения. В гражданском праве деньги и ценные бумаги также признаются вещью.

Выделение двух аспектов документа неявно означает их сравнительную независимость друг от друга. Документ характеризуется совокупностью параметров, одна часть из которых отражает информационную сторону документа, другая — вещную. Разумеется, эти параметры взаимосвязаны, но локализованы. Параметры АнД как предмета

достаточно очевидны. К ним можно отнести структуру, размеры, форму, цвет бумаги, шрифт, почерк, стиль графического размещения текста, цветовой фон, способ печати и другие. Эти параметры инвариантны к собственно информации, постоянны в широком диапазоне варьирования смысла, сущности, содержания документа.

Указанные вещные характеристики — это часть подмножества атрибутов в модели документа в виде множества. К атрибутам относятся и другие параметры, традиционно называемые реквизитами аналогового документа. Большинство из них также инвариантно к информации и может быть причислено к вещным параметрам, но некоторые отражают сугубо информационный аспект и должны быть включены в содержание как служебная (справочная) информация, в частности информация, идентифицирующая прохождение и исполнение документа. Список возможных реквизитов аналогового документа регламентируется ГОСТом 6.30-97 «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов» [31].

Можно утверждать, что вещный аспект аналогового документа отражается его атрибутами. Мы уже отмечали, что, фигурально выражаясь, атрибуты документа играют роль той материальной «коробочки», которая упаковывает нематериальную и бесплотную информацию, названную нами содержанием АнД: обеспечивает ее целостность, доступность, сохраняет конфиденциальность, позволяет аутентифицировать, придает ей индивидуальность оригинала или копии. Так что подобный вывод имеет достаточные предпосылки, как физические, так и смысловые.

Информационный аспект аналогового документа «спрятан» в графике знаков и далеко не так очевиден, как вещный. В аналоговой среде информационный и вещный аспекты физически связаны настолько прочно, что обычно их разделение невозможно. Применительно к электронному документу сразу возникает вопрос: «а где же “спрятана” вещь в ЭлД?».

Ведь электронный документ нельзя представить как предмет некоторой фиксированной формы, размеров, окраски и т. п. Более того, ранее показано, что даже говорить о фиксации активизированного ЭлД нельзя, а предмет всегда можно зафиксировать. Ответ на поставленный вопрос определяется задачами, решение которых обеспечивается вещной стороной документа.

Нас интересуют не физические характеристики документа, а совокупность прав по его использованию как вещи, что далеко не одно и то же. По гражданскому законодательству РФ как недвижимые вещи рассматриваются земельные участки, участки недр, обособленные водные объекты, леса, многолетние насаждения, здания, сооружения [7]. Выделение двух сторон документа фактически подразумевает два класса задач, решаемых в процессе документооборота, соответственно, в рамках информационного или вещного аспекта.

Из анализа аналогового документа как вещи следует, что вещный аспект электронного документа также должен также отражаться его атрибутами. Но здесь возникает вопрос, а чем существенным, с позиций объекта программно-технической среды, отличаются атрибуты от содержания документа при его отображении в электронном виде? В электронной среде, в отличие от среды аналоговой, физическая реализация атрибутов и содержания документа одинакова. Она представлена «одними и теми же» двоичными сигналами. Показано, что документ можно представить в виде множества элементов и что информация, содержание, выделяется маркировкой, окраской элементов некоторого подмножества этого множества. Для аналоговой среды принципиально, что маркировка производится самим субъектом, воспринимающим документ, выполняется на неформальной основе, базируясь на накопленных им знаниях.

Объект электронной среды знаниями не обладает, поэтому маркировка элементов подмножества как содержания задается заранее внешней силой. Сами по себе объекты электронной среды не могут

отличить атрибуты от содержания, компьютер не понимает «смысла, знания» — отличительной характеристики информации в мире человека. Все более и более изощренные алгоритмы обработки электронных сигналов лишь имитируют мышление, так же, как «умное» лицо студента иногда имитирует понимание лекции. Машине все равно, содержание или атрибуты она преобразует, ведь и различные виды атрибутов ЭлД также маркируются извне, например, позиционированием или специальной последовательностью символов начала и конца отображения атрибута.

Так что в общем случае электронный документ представляет собой последовательность, состоящую из окрашенных различным образом «кусков», причем «цвет» кусков, вообще говоря, не имеет значения, так как определяется априорным соглашением субъектов-участников электронного взаимодействия. Поменяем соглашение, поменяется маркировка, и то, что ранее считалось «содержанием», машина будет интерпретировать как некий атрибут, и наоборот. С позиций объектов электронной среды, в электронном документе отсутствует качественное отличие между содержанием и атрибутами. В зависимости от конкретной постановки задачи можно считать документ либо вещью, либо информацией.

В электронной среде половинчатое мнение не существует, среда допускает только однозначный ответ. Если решается задача передачи документа в условиях помех, то ЭлД можно считать информацией. Но если рассматриваются правовые аспекты, то вещный аспект электронного документа явно доминирует над информационным аспектом. Электронный документ можно интерпретировать как некоторое изделие, пусть и в весьма специфической форме, состоящее из системы взаимно увязанных и качественно однородных блоков и деталей. Формально (а в электронной среде неформальных подходов не бывает!) обработка ЭлД не требует сохранения информации, смысла, но требует обеспечения (вычислимой) изоморфности преобразований фрагмента, маркированного как

содержание ЭлД. *Электронный документ имеет значительно большие основания считаться только вещью, чем АнД.*

3.3.2. Возможность применения норм вещного права в сфере электронного взаимодействия

Правовые нормы в сфере электронного взаимодействия должны регулировать общественные отношения между субъектами, причастными к обмену электронными документами. Правоотношения субъектов, взаимодействующих при помощи ЭлД, целесообразно рассматривать в рамках вещного права.

Вещное право — субъективное гражданское право, объектом которого является вещь. Лицо, обладающее вещным правом, осуществляет его самостоятельно, не прибегая к содействию других (обязанных) лиц. Собственник вещи владеет, пользуется и распоряжается ею по своему усмотрению в пределах, установленных законом [7].

В правовом пространстве электронное взаимодействие можно интерпретировать как отчуждение прав собственности, владения, распоряжения и пользования электронным документом от одного субъекта к другому. В общем случае к технологическому циклу электронного взаимодействия причастны следующие категории лиц: Автор, Отправитель, Исполнитель, Получатель и/или Пользователь электронного документа. Не всегда Отправителем документа является Автор, а Получателем — Пользователь, так что взаимодействие субъектов отражается цепочкой: Автор/Отправитель — Исполнитель — Получатель/Пользователь.

Создание ЭлД осуществляется субъектом-Автором в электронной среде. Ранее было показано, что, поскольку человек находится вне рамок электронной среды, электронный документ может быть сформирован только из уже имеющихся в электронной среде «заготовок»: элементарных документов (знаков) и/или ранее сформированных иных входных

документов. Роль субъекта-Автора заключается в задании машине множества входных ЭлД, правил (алгоритмов) выбора из него нужных входных документов, алгоритмов формирования требуемого выходного документа на основе обработки и преобразования выбранных входных ЭлД.

Если автор создает оригинальный документ, то он формируется компьютером из множества элементарных, «маленьких» документов, отображающих алфавитные и цифровые знаки. Если документ создается на основе компоновки хранящихся в ЭВМ фрагментов, то во множество входных документов включаются эти фрагменты. Например, документы, сопровождающие процесс получения денег в банкомате, имеют стандартную форму. Они создаются посредством выбора из уже имеющихся в машине «заготовок» и последующей корректировки последних, процесс запускается при вводе автором карточки в банкомат, наборе соответствующего пин-кода и запрашиваемой суммы.

В любом случае автора можно считать собственником созданной им вещи — документа; он имеет право *владеть, пользоваться и распоряжаться* принадлежащим ему документом по своему усмотрению и в своих интересах непосредственно в пределах закона и независимо от воздействия других лиц. Кстати, компьютерные вирусы препятствуют реализации прав собственности автора, и потому их изготовление, реализация и распространение являются противозаконными.

Формирование документа происходит при использовании программно-технических средств, принадлежащих, в общем случае, не автору, а другому лицу, физическому или юридическому, будем называть его Исполнителем. Да и входные документы, хранящиеся в машине, принадлежат Исполнителю на правах собственности или владения. В правовом плане Исполнитель оказывает Автору услугу по изготовлению ЭлД по «чертежам и плану Автора». В свою очередь, по завершении создания документа Автор как собственник отчуждает Исполнителю свое

право владения (но не собственности!) принадлежащего ему имущества — документа, обеспечивая возможность выполнения Исполнителем соответствующих поручений, например, в части хранения, передачи (перевозки) и доставки документа адресату, его защиты, копирования ЭлД и т. д.

Исполнитель может привлечь в качестве субподрядчиков других Исполнителей, отправляя документ Автора для выполнения соответствующих технологических операций, которые не может выполнить самостоятельно. Тогда Исполнитель выполняет функцию Отправителя документа, а субподрядчик — функцию Получателя. При взаимодействии отправитель играет роль Владельца документа и отчуждает все или часть делегированных ему прав владения в пользу субподрядчика. Но это, в принципе, не меняет сути дела, взаимодействие Автора и Получателя/Пользователя реализуется при посредничестве Исполнителя.

Выполнив поручения Автора, Исполнитель передает документ адресату. При этом Автор как собственник может передать право владения документом полностью или частично, тогда адресат становится Получателем документа. Либо право владения сохраняется за Автором, и адресату отчуждается, полностью или частично, только право пользования ЭлД, тогда адресат является Пользователем документа. Применение электронного платежного поручения основано на передаче права владения, Получатель как владелец имеет возможность (после исполнения поручения) аннулировать или погасить документ, чтобы он не использовался вторично. ЭлД многократного действия, например, текст закона, предоставляется только в пользование, воздействовать на документ Пользователь не имеет право.

Приведенная схема взаимодействий субъектов посредством электронного документа намеренно упрощена, но позволяет выделить концептуальные положения в правовых аспектах электронного

взаимодействия. Подход с позиций вещного права обеспечивает правовую досягаемость электронного документа в течение всего жизненного цикла: всегда можно выделить конкретное юридическое или физическое лицо, отвечающее за текущую ситуацию электронного взаимодействия. Разумеется, многообразие возможных ситуаций не позволяет регулировать отношения участников взаимодействия только в рамках публичных договоров и публичного права, в ряде случаев необходимы персонифицированные договора и соглашения непосредственно между ними. Но основная масса вопросов может быть «снята» хорошо отработанными публичными нормами.

Приведем в качестве иллюстрации два полярных примера «машинного» и «ручного» создания ЭлД: актуализация счета клиента и формирование письма. Практически любая схема создания электронного взаимодействия может быть представлена как их композиция.

Собственником и владельцем электронного расчетного счета клиента является банк. Актуализация счета формально есть создание *нового* ЭлД, иначе приходим к абсурдной возможности изменения документа в течение жизненного цикла. Собственником и владельцем электронного платежного поручения является клиент, который, оставаясь собственником, отчуждает свое право владения и передает его банку. Банк, не являясь собственником поручения, не вправе его менять, но может им пользоваться, распоряжаться, аннулировать.

Операции, которые должны быть выполнены с переданными во владение банку входными электронными документами, заданы банком в прикладной программе. Например, «копировать определенные позиции в поручении, найти счет, вставить эти позиции на заданные места в счете, выполнить арифметические операции, погасить поручение». В результате формируется *новый* выходной ЭлД — актуализированный счет, собственником и автором которого является уже банк. Весь цикл

формирования происходит в рамках электронной среды, не требуется восприятия ЭлД субъектом-человеком.

При «ручном» создании ЭлД-письма процесс реализуется итеративно. Пусть автором уже сформирован фрагмент текста — являющийся его собственностью входной ЭлД-фрагмент. Автор, используя находящиеся в его распоряжении инструментальные средства, очередным нажатием клавиши создает еще один принадлежащий ему входной документ: ЭлД-знак. Далее Автор применяет находящийся в его пользовании объект электронной среды, текстовый процессор, который дополняет входной фрагмент знаком и создает *новый*, выходной фрагмент. Новый фрагмент также принадлежит автору, поэтому процесс можно повторить, пока не будет сформирован итоговый документ, который по построению является собственностью автора. И здесь можно не выходить за рамки электронной среды, аналоговое отображение создаваемого документа на мониторе формально не является необходимым.

Итак, мы приходим к следующим выводам.

Созданный субъектом-Автором ЭлД является его собственностью и его владением. Собственник ЭлД несет ответственность в рамках закона за его содержание.

В правовом смысле для реализации электронного взаимодействия достаточно допустить отчуждение прав владения или пользования (полностью или частично) от прежнего Владельца к новому Владельцу или Пользователю.

Пользователь не имеет прав владения документом, и, следовательно, не имеет права модифицировать документ.

При переходе ЭлД от Собственника к Владельцу должны отчуждаться только права владения, но не права собственности. Новый Владелец не может менять определенные фрагменты ЭлД. То, что обычно понимается под «содержанием и обязательными реквизитами» документа, это право собственности. Передав права владения другому Владельцу,

Собственник также утрачивает право коррекции отчужденного ЭлД. Соблюдение прав собственности и владения документом гарантирует отсутствие искажений в ЭлД в течение жизненного цикла. При нарушении прав собственника и/или владельца обеспечивается правовая платформа для предъявления претензий нарушителю.

Процедура отчуждения ЭлД от одного Владельца к другому может быть неоднократной. Правовая платформа для сохранения потребительских свойств документа в таком случае обеспечивается при выполнении следующего положения.

Владелец-отправитель несет ответственность за характеристики ЭлД перед Исполнителем, а Исполнитель — перед Владельцем-получателем.

Для ЭлД-оригинала положение очевидно, более сложной кажется ситуация передачи «копии» хранящегося ЭлД. На самом деле, процедура формирования ЭлД-копии, по существу, подобна созданию ЭлД-оригинала. Собственником при передаче Владельцу ЭлД-оригинала предоставляется право копирования в рамках Закона и/или соответствующего соглашения. Право копирования — это право изготовления на основе единственного входного ЭлД *нового* документа, называемого ЭлД-копией. При этом должны быть одинаковы фрагменты входного (оригинал) и выходного (копия) документов, называемые «содержанием».

С правовой точки зрения это разные документы: ЭлД-копия есть собственность Владельца ЭлД-оригинала, но не Автора; ЭлД-копия по сравнению с ЭлД-оригиналом имеет дополнительные атрибуты, отличные от первоисточника, позволяющие аутентифицировать не только Автора оригинала, но и Владельца-создателя копии, и т. д. Фактически мы имеем дело с определенным расширением авторского права. Авторское право есть объект гражданских прав, хотя Законом [35] и не распространяется в явном виде на документы.

Собственником ЭлД-копии является Владелец ЭлД-оригинала. Владелец ЭлД-оригинала несет ответственность в рамках закона за ЭлД-копию.

Электронный документ есть результат некоторой работы или услуги, оказываемой Исполнителем в рамках закона Владельцу(ам) ЭлД. Исполнитель не имеет права распоряжения и пользования ЭлД.

При отчуждении ЭлД правовые отношения между Владельцем(ами) и Исполнителем должны регулироваться соглашением (в том числе, публичным договором).

Исполнитель ЭлД несет ответственность перед Владельцем(ами) ЭлД и законом за согласованные с Владельцем(ами) объем и качество работ по изготовлению и сопровождению ЭлД.

Из предыдущего становится очевидным, сколь многогранными могут быть правоотношения субъектов, причастных к реализации электронного взаимодействия. Здесь взаимоотношения заказчика и исполнителя, потребителя и изготовителя, компаньонов и посредников и др. Конечно, когда сектор действенности электронного документа ограничен рамками одного юридического лица, например, в корпоративных информационных системах, то правовое регулирование возможно административным путем. Но уже в близкой перспективе примет массовый характер межкорпоративное электронное взаимодействие. Дальнейшее успешное регулирование этой сферы на основе административных методов явно проблематично.

Создание специализированной нормативно-правовой базы требует не только значительных ресурсов, но, самое главное, большого времени для шлифовки ошибочных, неоднозначных или неконкретных положений, что в условиях беспрецедентных темпов развития информационных технологий недопустимо. Проведенный анализ разрабатываемых федеральных законопроектов достаточно убедительно подтверждает этот тезис. Целесообразным является отнесение электронного документа к

одной из известных юридических категорий, что позволило бы использовать наработанную и отшлифованную многолетним применением правовую базу, разумеется, с уточнениями, отражающими принципиальную специфику электронного документа.

При анализе дуализма документа показано, что вещный аспект электронного документа существенно значимее, чем такой же аналогового. Установлено, что при электронном взаимодействии отношения субъектов достаточно адекватно моделируются передачей (отчуждением) прав собственности, владения, пользования от одного субъекта другому. Действующий Федеральный закон «Об информации, информатизации и защите информации» от 20.02.95 г. [23] предусматривает «…право собственности на отдельные документы и отдельные массивы документов». В статье 6 Закона информационные ресурсы рассматриваются как элемент состава имущества и объект права собственности юридических и физических лиц. Устанавливается, что информационные ресурсы могут входить в состав имущества, быть товаром.

Вытекающие из концепции действующего Закона [23] и развитые в настоящем разделе положения дают веские основания считать, что, с непринципиальными ограничениями, электронный документ можно рассматривать как объект гражданских прав. Преимущества применения развитой юридической базы столь велики по сравнению с созданием специального правового обеспечения электронного взаимодействия «с нуля», что подобная правовая интерпретация, какой бы спорной она не казалась на первый взгляд, должна быть тщательно исследована специалистами.

Объекты гражданских прав (ОГП) — материальные и нематериальные блага, по поводу которых возникают гражданские правоотношения. Согласно ст. 128 ГК РФ к ОГП относятся вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные

права; работы и услуги; информация; результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность); нематериальные блага. Объекты гражданских прав могут свободно отчуждаться или переходить от одного лица к другому в порядке универсального правопреемства (наследование, реорганизация юридического лица) либо иным способом, если они не изъяты из оборота или не ограничены в обороте [7].

Любой ЭлД уникален, не может существовать идентичных ЭлД, нескольких экземпляров ЭлД. Таким образом, документ определяется однозначно, ЭлД находится в собственности, владении, пользовании субъекта, по поводу ЭлД возникают гражданские правоотношения, связанные с переходом от одного Владельца к другому. Если ЭлД не изъят или не ограничен в обороте, то документ может свободно отчуждаться или переходить от одного лица к другому, в том числе в порядке универсального правопреемства.

Можно также считать, что публичные электронные документы обладают свойством *оборотоспособности*, документы с ограничением доступа, конфиденциальные, секретные документы — *ограниченной оборотоспособностью*. Возможность перехода от одного владельца другому правовых, управленческих, коммерческих ЭлД ограничивается, что должно быть законодательно уточнено.

Оборотоспособность — свойство объектов гражданских прав (ОГП), заключающееся в возможности их перехода от одного лица к другому по договору купли-продажи, мены или дарения либо в порядке универсального правопреемства (в форме наследования или реорганизации юридического лица). ОГП делятся на три группы: *свободно обращающиеся* объекты; *ограниченные* в обращении; *полностью изъятые* из оборота. Свободное обращение ОГП — общее правило, а ограничение и тем более полное изъятие из оборота — исключение. Ограничение оборотоспособности выражается в том, что соответствующие виды

объектов могут принадлежать только государственным организациям, либо только гражданам и юридическим лицам РФ, либо находиться в обороте только по специальным разрешениям.

3.3.3. Защита информации как защита прав субъектов-участников электронного взаимодействия

Аналоговый документ — продукт простых технологий в том смысле, что процесс изготовления и результат, готовый АнД, исчерпывающе могут контролироваться субъектом. Создание АнД почти всегда возможно непосредственно человеком при помощи «пера и бумаги» или пишущей машинки. Создание и существование электронного документа — изготовление, обработка, передача, хранение и т. д. — возможны только в структурно-сложной пространственно разделенной системе сложных технических и программных средств. В технологическом плане электронный документ является сложным изделием.

Чем крупнее система, тем большее количество субъектов причастно к ее созданию, функционированию и обслуживанию. Чем сложнее система, тем большее число неконтролируемых факторов влияет на конечный результат, тем труднее диагностика и идентификация нежелательных воздействий, их предотвращение. Чем обширнее система, тем большее число точек несанкционированного доступа она имеет, тем выше вероятность повреждения ее продукции — электронного документа, и ее услуг — реализации электронного документооборота между участниками информационного взаимодействия.

В электронном взаимодействии участвуют, с одной стороны — безответственная техническая система, с другой стороны — субъекты правоотношений, пользующиеся продукцией и услугами этой системы, функционально связанные с этой системой. Связь между субъектами, причастными к реализации электронного взаимодействия, и электронным документом как продукцией технической системы определяется

выполнением требований к качеству продукции, имеющих технологический характер — машина только исполняет предписания ее владельцев и пользователей. Основным критерием должного качества является *достоверность электронного документа* — совокупность свойств ЭлД, обеспечивающих его признание в рамках сектора действенности (юридическим) фактом.

Изготовление и сопровождение электронного документа обеспечивается последовательностью конкретных преобразований входных ЭлД. Если каждое преобразование ЭлД — достоверное преобразование, то при достоверных входных документах и выходной документ достоверен. Приходим к понятию *достоверной среды* существования ЭлД как совокупности программных и технических средств, обеспечивающих только достоверные преобразования ЭлД, гарантирующие достоверность выходного (преобразованного) документа, если входной ЭлД достоверен.

Ранее было установлено, что для признания документа фактом, в общем случае, должны обеспечиваться:

- индикация целостности документа;
- доступность содержания документа объектам сектора действенности;
- недоступность содержания документа объектам иных, априорно заданных, секторов действенности (конфиденциальность);
- аутентификация автора и/или отправителя документа;
- аутентификация получателя и/или адресата документа;
- аутентификация маршрута (промежуточных точек) прохождения документа от отправителя до получателя;
- кратность применения документа.

Именно в этом и заключается назначение мероприятий, традиционно понимаемых как защита информации. С другой стороны, нарушение целостности ЭлД есть порча «чужой вещи»; несанкционированный доступ,

нарушение конфиденциальности — неправомерное пользование чужой собственностью; невозможность аутентификации, дискредитация ЭлД — нарушение исключительных прав на ЭлД, прав авторства, прав на имя, деловой репутации и пр. Исполнитель ЭлД несет ответственность перед Владельцем ЭлД и законом за согласованное с Владельцем качество (достоверность) принадлежащего ему фрагмента электронной среды существования.

В действующем Федеральном законе «Об информации, информатизации и защите информации» [23] обеспечение прав субъектов в информационных процессах определяется как одна из целей защиты информации. Следовательно, правоотношения между субъектами, причастными к электронному взаимодействию посредством неодушевленного и не воспринимаемого человеком электронного документа, должны определяться гражданскими правами этих субъектов: имущественными и связанными с ними личными неимущественными отношениями. Таким образом, можно дать эквивалентное определение качества ЭлД.

Качество ЭлД — совокупность свойств ЭлД как изделия, обеспечивающих реализацию прав субъектов электронного взаимодействия: собственности, владения, пользования, распоряжения.

Так как «содержание» документа постоянно в процессе его изготовления и сопровождения, а изменение качества есть изменение защищенности ЭлД, то воздействие на качество возможно при изменении либо параметров среды существования, либо атрибутов документа. Качество ЭлД определяется средой его существования и атрибутами документа. Для изготовления и сопровождения документа необходимы сложные средства, созданные третьими лицами, так что даже добросовестный Исполнитель не может гарантировать Владельцам должного качества изготовления и сопровождения ЭлД. Такие требования

подлежат взаимному согласованию, распределение ответственности должно регулироваться соглашениями между участниками.

Назначением защиты информации является обеспечение прав субъектов, принимающих участие в реализации электронного взаимодействия.

3.4. Выводы

1. Жизненный цикл сообщения или документа протекает в трех средах существования. Внешняя образована социальной средой, подмножество мыслящих субъектов которой формирует сектор действенности документа. Документ должен быть предъявлен социуму, социальное назначение документа нематериально. В рамках сектора действенности документ признается информационным фактом. Остальные две среды имеют дело не со «знанием» и «сведениями», но с *материальным* отображением информации в виде изделия: аналоговой — в виде предмета; активной электронной — в виде процесса. Документ определяется как пара: сектор действенности и отображение информации, оформленное в соответствии с правилами сектора действенности.

Документ является сообщением о факте, которое признается в рамках сектора действенности легитимным основанием для сохранения, изменения, прекращения определенных взаимоотношений между членами сектора.

2. Необходимым и достаточным условием для того, чтобы документ выполнял роль информационного факта, является его демонстрация. *Демонстрация — это предъявление по требованию сектора действенности в нужном месте и в нужном момент изделия-носителя информационного факта для того, чтобы с него были сняты предложенным сектором действенности способом параметры изделия — характеристики информации.*

3. Изделие-документ характеризуется двумя группами параметров: основные, условно-переменные — отражающие содержание; вспомогательные — условно-постоянные. Сектор действенности, предписывая технологию изготовления документа, задает ряд эталонных параметров, значения которых являются необходимым условием отсутствия искажений содержания.

Демонстрация информационного факта предполагает, что заданный сектором действенности ряд физически измеримых параметров изделия ***совпадает с параметрами эталона****, существовавшего в исходной точке.* Только тогда, когда в выполнении этого требования сектор действенности *убежден*, возникают достаточные основания для признания сообщения *документом*, закрепляющим информацию о (юридическом) факте.

4. Базисными требованиями к материальной реализации документа являются доступность, целостность, легитимность.

Доступность — физическая возможность измерения заданных параметров изделия-документа (содержания, атрибутов, технологии) предписанными сектором действенности средствами в заданных точках «пространство-время» в течение конечного времени с момента возникновения потребности в демонстрации.

Целостность — при любой демонстрации изделия-документа эталонные значения заданных сектором физических параметров демонстрируемого документа-изделия должны лежать в заданном допуске соответствующих параметров атрибутов документа в начальной точке жизненного цикла.

Легитимность — демонстрируемый документ (как изделие) должен содержать параметры, объективно подтверждающие правомерность использованных на протяжении жизненного цикла документа технологий.

Каждое базисное требование к документу дополняется требованием к сектору. Дополнительные требования выглядят следующим образом:

- **доступность** (параметров сообщения) – **конфиденциальность** (для подмножества субъектов сектора);
- **целостность** (параметров сообщения) – **инвариантность** (других параметров с точки зрения сектора);
- **легитимность** (применяемых технологий) – **вариабельность** (других технологий с точки зрения сектора).

5. Собственно информация нематериальна, но отображение информации должно быть предъявлено в материальном виде изделия. *Отображение информации есть заданное сектором действенности и считываемое в определенном порядке множество (совокупность) физически измеримых параметров изделия-носителя*: предмета, зафиксированного в пространстве; процесса, зафиксированного во времени. Само изделие служит объективной платформой для определения порядка на множестве параметров. *При информационном взаимодействии должно сохраняться отношение упорядоченности множества сигналов, маркированного как «информация», должен обеспечиваться (вычислимый) изоморфизм преобразований.*

6. В общем случае изделие-носитель D, находящееся в пространстве X и времени T, интерпретируется как функция $D(x, t)$ значений аргументов в окрестности χ точки пространства x и в интервале τ момента времени t. Возможны два предельных случая:

- изделие-носитель D сообщение от t не зависит $D(x, t) = D(x)$. Отображение информации одинаково в **любой момент** времени, сосредоточено только в конечном объеме χ пространства — изделие в виде *предмета*.
- Изделие-носитель D сообщение от x не зависит $D(x, t) = D(t)$. Отображение информации существует только в окрестности τ точки t,

но зато оно присутствует во **всех точках** пространства X — изделие в виде *процесса*.

7. Для окружающего нас мира базовыми являются две материальные категории существования — материя и энергия. Это равноправные категории описания реального мира в том смысле, что одна не является следствием другой, в математике говорят — базисные аргументы. Предмет есть пространственная конструкция, тогда как сигнал — временная. Это означает, что потенциально для отображения информации могут использоваться:

- пространственное изменение физических параметров *материи*, материального предмета, сосредоточенного в объеме *пространства* χ — традиционные технологии;
- временное изменение физических параметров *энергии*, материального сигнала, процесса, наблюдаемого в интервале *времени* τ — активные электронные технологии.

8. Основное преимущество традиционных технологий — простота *перемещения во времени* изделия, *хранение* документа или сообщения. Недостатком применения предмета (материи) в качестве носителя является низкая скорость перемещения документа в пространстве. Достоинство электронной технологии — легкость *перемещения информации в пространстве*, *передача* документа. Недостаток применения процесса (энергии) в качестве носителя — в перемещении документа во времени, энергия быстро рассеивается.

9. Оптимальным решением с позиций экономики является тот случай, когда технология предусматривает в передаче форму сообщения в виде сигнала, а во время хранения — предмета. Это новые информационные технологии. Их кардинальное отличие от традиционных информационных технологий заключается в том, что они базируются на **изготовлении** документа для его демонстрации перед субъектами (объектами) сектора действенности. Концептуальные свойства НИТ можно

получить из общего представления документа как демонстрируемого явления, включая анализ таких категорий демонстрации как «пространство и время», «материи и энергии», «предмет и процесс».

10. Документ имеет двойственную природу. Дуализм документа проявляется в том, что: документ может рассматриваться как информация; документ может рассматриваться как вещь, предмет — нечто, на чем эта информация «закреплена». Вещный аспект электронного документа доминирует над информационным аспектом. В технологическом плане электронный документ есть сложное изделие. Правовые нормы в сфере электронного взаимодействия должны регулировать общественные отношения между субъектами, причастными к обмену электронными документами. В число их входят не только непосредственные участники информационного обмена, но и все субъекты-посредники, имеющие возможность воздействия на технологическую реализацию электронного документооборота.

11. В правовом пространстве электронный документ в процессе технологической реализации электронного взаимодействия может рассматриваться как объект гражданских прав. В общем случае в технологическом цикле электронного взаимодействия участвуют следующие категории лиц: Автор, Отправитель, Исполнитель, Получатель и/или Пользователь электронного документа. Электронное взаимодействие можно интерпретировать как отчуждение прав собственности, владения, распоряжения и пользования электронным документом от одного субъекта-участника к другому.

12. Назначением защиты информации является обеспечение прав субъектов, принимающих участие в реализации электронного взаимодействия. Правоотношения между субъектами, причастными к электронному взаимодействию посредством неодушевленного и не воспринимаемого человеком электронного документа, должны

определяться гражданскими правами этих субъектов: имущественными и связанными с ними личными неимущественными отношениями.

Глава 4. КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ АППАРАТНОЙ ЗАЩИТЫ ТЕХНОЛОГИИ ЭЛЕКТРОННОГО ОБМЕНА ИНФОРМАЦИЕЙ

4.1. Обоснование возможности аппаратной защиты электронного обмена информацией

Результаты, полученные в предыдущих разделах работы, определяют представленную на рис. 3.1 схему электронного обмена информацией и позволяют сформулировать следующие предпосылки концептуальной модели аппаратной защиты.

1. Жизненный цикл электронного документа протекает в трех средах существования, вложенных одна в другую. Внешняя оболочка образована социальной средой, подмножество мыслящих субъектов которой формирует сектор действенности документа. Среда, но не отдельный субъект, диктует правила обмена информацией своим членам-субъектам. Выделяются два класса правил — семантические и технологические. Семантические правила определяют требования, гарантирующие, в рамках *социальной среды*, однозначность интерпретации *информации* (содержания) документа как сведения, смысла, знания. Технологические правила определяют требования, гарантирующие, в рамках *сектора действенности* документа, наличие формальных предпосылок для признания его (юридическим) фактом.

Семантические правила определяют требования к языку (тезаурусу) документа, стилю изложения, грамматике, синтаксису и др. Классический пример – сообщение «казнить нельзя помиловать» с пропущенной запятой не может быть содержанием документа. Текст искового заявления в российский суд нельзя писать на китайском языке. Семантические требования — прерогатива социальной среды, их соблюдение участниками взаимодействия поощряется, а невыполнение наказывается в рамках общественных, производственных отношений между субъектами сектора действенности.

В электронной среде информация не имеет смысла и трактуется как множество с заданным на нем отношением порядка, поэтому выполнение семантических требований и, соответственно, семантических правил *не входит* в число функциональных задач защиты электронной информации.

Технологические правила определяют требования к технологии формирования, обработки, передачи и хранения информации в течение жизненного цикла документа. *Сектор действенности документа предписывает*, чтобы используемая технология необходимо обладала рядом специальных, заданных сектором характеристик. По существу, налагаются ограничения на процессы отображения информации в течение жизненного цикла документа: изготовления, обработки, передачи и хранения документа.

Только когда все требования выполняются, возникают достаточные основания для признания сектором информации *документированной*, а сообщения — документом, т. е. сообщением, закрепляющем возникновение юридического факта. ***Не зафиксированная информация, а информация, фиксирующая (закрепляющая) факт!*** Только тогда прямые участники (автор, адресат и др.) могут использовать документ как формальное основание для возникновения правоотношений, как между собой, так и с третьими лицами (субъектами социальной среды), а посредники приобретают право на оплату услуг за реализацию информационных технологий. Достигается цель защиты информации — обеспечение прав субъектов, принимающих участие в реализации электронного взаимодействия.

2. Электронное взаимодействие обеспечивается *совместно* элементами как электронной, так и аналоговой среды. ЭлД в активизированном состоянии есть *процесс* и является элементом электронной среды, ЭлД в пассивном состоянии (на машинном носителе) есть *предмет* и является элементом аналоговой среды. Но точно то же самое можно сказать и о программе — по существу это документ, только содержащий информацию не о факте, а о процессе.

Природа как ЭлД, так и программы одинакова. Программа предназначена исключительно для применения в электронной среде, для запуска и регулирования цифровых процессов. Но и документ, если он не выходит за рамки электронной среды, инициирует только процессы. Например, при получении денег в банкомате создаваемые промежуточные ЭлД запускают и задают параметры процесса формирования последующих электронных документов в технологическом цикле обслуживания клиента.

Если ЭлД должен храниться или использоваться как средство взаимодействия субъектов в аналоговой среде, то по умолчанию неизбежно его преобразование в аналоговую форму. Текст может быть написан буквами на поверхности листа бумаги, светящимися точками — на экране монитора, но может быть «написан» и ориентацией доменов на поверхности магнитного носителя. Аналогично можно говорить и об аналоговой форме существования программы.

Приходим к положению о неразрывной связи электронной и аналоговой среды. Понимая электронную среду существования как множество элементов, взаимодействующих на основе однозначных, формальных правил обработки, хранения и передачи цифровой информации, надо учитывать, что сами эти элементы реализованы в объектах аналоговой среды, характеризующихся как пространственной, так и временной непрерывностью. Любой аналоговый объект принципиально вариативен, его параметры не могут быть измерены точно, к тому же они изменяются с течением времени. Установление неизменности аналогового объекта за конечное время с использованием конечных ресурсов *всегда* возможно лишь с конечной точностью. Аппаратную защиту можно рассматривать как своеобразный интерфейс между электронной и аналоговой средой. Модуль защиты, с одной стороны, есть изолированный материальный объект, тогда как с другой, в активном состоянии, это цифровой процесс. Существенным является, что и ЭлД, и программа — элементы электронной среды, в то время как аппаратный модуль — аналоговой. Внутреннее противоречие,

изначально заложенное в таком разделении, неизбежно приводит к своеобразию формальной модели аппаратной защиты.

3. Ограничиваясь технологическим аспектом информационного обмена, мы, тем самым, выходим из социальной среды и погружаемся в среду физического существования электронного документа: в виде *предмета* в аналоговой среде, в виде *процесса* в цифровой (электронной) среде. Отличие процесса и объекта имеет системный характер, поэтому в безопасности электронного информационного обмена выделяются два качественно разных направления: защита предмета, т. е. собственно отображения информации; защита процессов преобразования — технологий, *инвариантных* к защищаемой информации.

Первое направление характерно для статической формы представления информации физическими свойствами объекта. Информация *фиксируется* параметрами предмета, которые необходимо должны быть постоянны в течение жизненного цикла документа, причем доступ к их измерению (наблюдению) ограничивается. В этом случае говорят о *защите информации*, понимая защиту предмета-носителя от повреждения и от несанкционированного доступа. Такая форма представления информации *доминирует* в аналоговой среде существования документа, хотя имеет место и в электронной среде, например, в случае хранения ЭлД в устройствах памяти.

Методы защиты зафиксированной аналоговой информации, *информации-предмета*, отработаны теорией и практикой применения традиционных аналоговых документов: носитель должен быть защищен от несанкционированного доступа. С этих позиций *защита электронного документа в аналоговой форме существования* не имеет существенных особенностей по сравнению с традиционными аналоговыми документами и поэтому далее не рассматривается. Стандартное возражение, что, в отличие от бумажного документа, информацию на магнитном носителе несравненно проще подменить «незаметным» способом, неправомерно: чтобы стереть или

изменить информацию на диске принципиально необходимо перейти к динамической форме существования информации — в виде *информации-процесса*. Это абсолютно иная форма существования документа, доминирующая в электронной среде, и здесь действуют иные законы — з*ащищается не информация*, *но технология* отображения информации в виде процесса.

И в аналоговой среде информация как сведение не всегда представлена в статической форме, имеет место и динамическая форма отображения в виде процесса. Например, зашифрованное сообщение приобретает смысл только в *процессе* расшифровки, т. е. в жизненном цикле документа принципиально должен быть динамический этап. Акценты защиты информации радикально меняются: например, *не нужно* защищать криптограмму (точнее, объект-информацию) от НСД, а надо предотвратить доступ к ключу шифрования — элементу *технологии* шифрования, никак *не зависящему* от защищаемой информации.

4. Для традиционного документа характерна форма существования информации в виде объекта. Исторически такой подход доминирует в общественном сознании и в случае электронного обмена информацией. Активизированный ЭлД существует только в форме процесса, поэтому в электронной среде *доминирует* защита процессов преобразования информации. Информация индицируется регистрацией изменений характеристик некоторого физического процесса в заданных точках пространства в течение конечного временного периода. Сам процесс описывается детерминированным алгоритмом, так что при любом процессе на входе устройства преобразования всегда можно *однозначно* предсказать процесс на выходе. Преобразование информации-процесса является *допустимым* (санкционированным), если оно отвечает технологическим требованиям сектора действенности: если на входе допустимого преобразования — защищенная информация-процесс, то на выходе будет также защищенная информация.

В силу последовательного характера процессов в электронной среде совокупность (последовательность) допустимых преобразований образует допустимый протокол формирования, обработки или передачи информации, совокупность (последовательность) протоколов — допустимую технологию информационного взаимодействия. В достаточно широких пределах технология *инвариантна* к информации, не зависит от конкретной реализации информации-процесса. Применение допустимых технологий, отвечающих требованиям сектора, является достаточным условием гарантии защиты информации-процесса.

Выбор класса допустимых технологий — прерогатива *сектора* действенности документа, однако реализация технологии — обязанность отдельных *субъектов*, владеющих средствами ВТ и/или обеспечивающих технологическое сопровождение информационного обмена. Противоречия между общим и частным — сектором и субъектом, коллективом и его членами, потребителем и производителем, государством (если документ признается юридическим фактом) и личностью — неизбежны. Поэтому фактически использованная технология не всегда является допустимой. В этом случае возможно нарушение защиты информации-процесса, ошибочное признание сектором сообщения документом.

5. Содержанием комплекса мероприятий, понимаемых как защита ЭлД-процесса, является *не защита данных, а защита допустимости технологии*, применяемой при физической реализации документа в виде объекта или процесса. Если технология допустимая — отвечает требованиям сектора действенности, то информация признается защищенной, если нет — вопрос открытый. Сразу встает вопрос, а как отличить допустимую технологию от недопустимой? И, если в момент поступления входной информации-процесса выбрана допустимая технология, то как обеспечить ее сохранение в течение всего времени преобразования, гарантирующего защищенность выходной информации-процесса? И вообще, неизменность (постоянство) чего именно

надо обеспечивать, ведь технология есть процесс, принципиально меняющийся во времени?

Технология преобразования является фиксированной, постоянной, если при всякой ее реализации сохраняется априорно заданное однозначное соответствие между входным и выходным процессами (информацией).

В определении указаны три фактора — собственно технология, входной и выходной процесс, — так что в общем случае отделить описание технологии от преобразуемой информации нельзя: некоторые технологии можно задать *только* таблично. Однако такая ситуация нехарактерна для электронной обработки информации: при длине сообщения в n бит таблица соответствия должна содержать 2^n членов, т. е. реально длина входной информации-процесса не должна превышать десятка букв. Таким образом, почти всегда должен существовать универсальный способ описания технологии преобразования информации, не зависящий от преобразуемой информации.

И такое описание известно — *алгоритм преобразования*. В электронной среде алгоритм может быть задан двумя способами: *программно* — в виде *информации* об управлении процессом, совокупностью команд, зафиксированных в памяти в виде программы; аппаратно — в виде материального *объекта* с априорно заданными характеристиками выполняемого им преобразования, например, сумматор или регистр и т. п.

Ранее аналоговая форма отображения информации была определена как объект (носитель), наблюдаемые физические характеристики которого (буквы как раскраска поверхности) поставлены в однозначное соответствие с информацией. Следовательно, *аппаратную реализацию процесса можно также интерпретировать как аналоговый объект (устройство), физические характеристики которого (пара «сигнал на входе — сигнал на выходе») отображают информацию о процессе в устройстве*. Технически наблюдение физических характеристик устройства более сложно, чем

носителя аналоговой информации, но принципиального значения это не имеет.

6. Подобная интерпретация означает, что технологию преобразования информации и саму информацию можно рассматривать как объекты с одинаковым математическим описанием, с единых концептуальных позиций. При отображении информации выделяют компоненты: знак (буква), слово, фраза, абзац и так далее. Аналогично можно интерпретировать и компоненты технологии: отдельные операции образуют алфавит, алгоритм — слово, протокол — фразу, технология — текст. Конечно, информация-процесс и информация-технология — это разная информация, информация о разных явлениях.

Основное требование к защите информации — сохранение отношения упорядоченности знаков, символов (изоморфности). Основное требование к защите технологии — сохранение отношения упорядоченности отдельных операций, ее составляющих. Соответственно, нуждается в уточнении определение информационной технологии. Если ранее информационная технология понималась как [89]: «Приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных», то точнее будет дополнить это определение словом «последовательность», что бы подчеркнуть, что технология – это не «совокупность» применяемых в произвольном наборе «приемов», а фиксированная последовательность. Таким образом, «информационная технология – это *последовательность* приемов, способов и методов применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных». Подобная трактовка намечалась и ранее, однако логического развития не получила. В моделях гарантированно защищенной информации, анализ которых проведен в разделе 1.2.8, предлагалось систему $\sum$ описывать в форме слов некоторого гипотетического языка $Я$ над некоторым конечным алфавитом A. Объект в $\sum$ — это конечное множество слов из $Я$, состояние

объекта — выделенное слово из множества, определяющего этот объект. С понятием объекта связано агрегирование информации в ∑ и о ∑.

Установленное концептуальное единство обеспечивает единую теоретическую платформу решения проблемы информационной безопасности электронного взаимодействия: *для защиты информации-процесса достаточно защитить информацию-технологию*. Находится ответ и на нетривиальный, по тщательному размышлению, вопрос: почему для защиты информации приходится защищать от НСД совершенно посторонний объект, никак не зависящий от защищаемой информации — помещение, где стоит компьютер?

7. Отсюда автоматически вытекает общеизвестное положение, что *идеальная* защита ЭлД невозможна в принципе: для защиты информации-ЭлД необходимо защитить информацию-технологию. Всегда найдется более широкий фрагмент технологической среды существования информации, включающий предыдущий как подмножество. Но последнее предложение означает возможность повышения уровня защищенности объекта — смена рубежей защиты позволяет применять более эффективные методы и механизмы. Отличие технологии от ЭлД концептуально и заключается в априорной известности, заданности, неизменяемости технологии. С системных позиций, защищать фиксированный объект всегда проще, чем изменяющийся.

Итак, среда существования ЭлД, в свою очередь, может трактоваться как информация, представленная как в аналоговом (аппаратные средства), так и в цифровом, электронном (цифровые процессы) виде.

Так как аналоговая форма представления информации имеет несопоставимо более высокую избыточность, нежели цифровая (электронная), то потенциально защита аналоговой (аппаратной) формы представления процесса как элемента технологии принципиально намного эффективнее, чем электронной (программной). Таким образом, из теории следует, что *применение аппаратных средств защиты электронной среды*

существования документа — одно из наиболее перспективных направлений информационной безопасности. Причем, поскольку процесс как элемент технологии априорно известен, то его аппаратная реализация в принципе физически реализуема.

Такой же результат вытекает в силу известности, заданности технологии. Ее защита может быть реализована в общем случае более эффективно, так как сфера защиты много уже, чем в случае произвольной информации документа. Соответственно, для защиты технологии могут быть применены более специализированные методы, в частности, аппаратные.

8. Содержанием комплекса мероприятий, понимаемых как защита ЭлД, является как *защита информации*, так и *применение адекватной технологии* при физической реализации документа в виде объекта или процесса. Если технология отвечает требованиям сектора действенности, то информация защищена, если нет — вопрос открытый. Это существенное уточнение, противоречащее широко распространенному заблуждению, отразившемуся в используемой терминологии. Это различные, а в указанной выше трактовке — даже противоположные, задачи объединяются под одним названием — защита информации. Разграничивается доступ к *инструментальным средствам*, т. е. технологиям отображения ЭлД в виде процесса, а говорят о защите от НСД к *информации*. Аналоговый документ хранят в сейфе, защищают доступ в *сейф*, а говорят о конфиденциальности *информации*. *Секретен ключ* шифрования, не зависящий от информации, но говорят о *секретной информации*.

9. Сущность защиты любого объекта, будь то документ или технология, заключается в сохранении тождественности (в общем случае — взаимно однозначного соответствия) свойств этого объекта при его наблюдении в двух разных точках «пространство-время». Защита абсолютна, если *гарантируется*, что характеристики объекта, измеряемые в точке (x, y, z, t), точно такие же, как в эталонной точке (x_0, y_0, z_0, t_0). Защита отсутствует, если сопоставление характеристик невозможно: либо

неизвестны характеристики эталона в точке (x_0, y_0, z_0, t_0), либо невозможно измерить характеристики объекта в точке приема (x, y, z, t).

Для реализации любого уровня защиты необходима избыточность — известность не только результата, но и эталона. Должны быть известны, с той или иной погрешностью, характеристики объекта как в точке (x, y, z, t) наблюдения, так и в эталонной точке (x_0, y_0, z_0, t_0). Специфика собственно информации-документа и информации-технологии обусловливает и специфику методов их защиты. В первом случае известна фактическая информация, почти неизвестна эталонная. Во втором случае, известна эталонная технология, почти неизвестна фактически использованная.

10. Цифровая среда базируется на логических, детерминированных правилах преобразования, это среда точных процессов. Любое преобразование в электронной среде есть результат строго определенной безызбыточной последовательности процедур: удаление, введение или изменение хотя бы одной команды, как правило, полностью меняет результат. В то же время информация как сведение избыточна и потому обладает некоторой «внутренней» стойкостью к изменениям ее представления. Качественно более высокий уровень «жесткости» является существенным отличием «информации-технологии» от «информации-документа».

Механизмы и методы защиты собственно электронного «документа-информации» базируются на *случайности эталона и известности реализации*, тогда как защиты электронной «технологии-информации» — на *известности эталона и случайности реализации*. Эталонная технология определяется правилами сектора действенности документа и необходимо *фиксируется* на достаточно длительное время явными или неявными соглашениями участников. Выполняется объективная предпосылка использования аппаратных методов и механизмов защиты электронной технологии — фиксированность — необходимое условие подобной

реализации, неминуемо сопряженной с потерей универсальности, гибкости, адаптируемости, управляемости алгоритмов и процедур.

Поскольку в электронной среде нельзя зафиксировать процесс-документ, но можно — процесс-технологию, то *аппаратные методы защиты возможны в основном в части защиты «информации-технологии»*. Потенциал аналоговых методов и механизмов защиты несопоставимо выше, чем программных, поэтому аппаратная реализация процедур и алгоритмов, играющих ключевую роль в технологии электронного обмена информацией, позволяет качественно повысить уровень защищенности. Тем самым обосновывается предметная область настоящего исследования — *аппаратная защита технологии электронного обмена информацией*.

11. Характеристики надежности и живучести системы тесно связаны, но обозначают далеко не одно и то же. Надежность есть свойство системы сохранять способность выполнять *заданные функции в заданном* объеме, тогда как живучесть подразумевает просто способность выполнять *заданные функции*, не фиксируя, в каком объеме они выполняются. Одномоторный самолет надежней двухмоторного с двигателями такой же суммарной мощности — хотя бы за счет меньшего суммарного числа деталей в моторе. Но менее живучий — отказ мотора в первом случае ведет к катастрофе, тогда как во втором, обычно, к аварийной посадке.

Таким образом, целью защиты «документа-информации» можно считать повышение его надежности, тогда как цель защиты «технологии-информации» — обеспечение *живучести*. Акцент работ меняется, при защите технологии приходится обеспечивать защиту *всех* процедур на *всех* этапах работы вычислительной системы, а не только имеющих прямое отношение к обработке электронного документооборота — и в этом суть *мультипликативной парадигмы* защиты. Теоретически это вытекает из детерминированности алгоритмов, процедур, протоколов. На практике данное положение прекрасно иллюстрируется, например, необходимостью

защиты программной среды от вирусов, влияние которых на конкретный «документ-информацию» зачастую крайне неочевидно.

13. Абсолютная защита невозможна, всегда возможно нарушение защищенности объекта, проявляющееся в различии характеристик объекта и эталона в соответствующих точках наблюдения. Учитывая, что отсутствие информации много лучше, чем ложная информация, информация отклоняется, если нет достаточной уверенности в ее защищенности. Поэтому защищенность необходимо должна индицироваться, и, значит, *сопоставление с эталоном*, пусть неявное, необходимо должно осуществляться.

В составе ЭлД необходимо должны присутствовать «индивидуальные следы» использованной технологии. Необходимо гарантировать приемлемую для сектора действенности *вероятность* выполнения предписанных сектором требований к технологии информационного обмена. Гарантия может быть и неявной: если априорно известны применяемые технологии или если математическое ожидание ущерба от ошибочного придания сообщению статуса документа и, наоборот, документу — статуса сообщения, незначительно. Например, взаимодействие субъектов в специальной вычислительной сети или информационный обмен в локальной сети небольшой организации.

В противном случае гарантия должна быть явной, и тогда примененные технологии формирования, обработки, передачи, хранения документа необходимо должны *индицироваться*. Когда сектор действенности признает документ подлинным, а содержащуюся в нем информацию — сообщением о факте, то это означает, что на основе физической реализации документа можно установить, что требования сектора к данному виду документа соответствуют фактической технологии его изготовления. Подлинность банкноты подтверждается производством в заданном классе технологий, но не ее номиналом; криптографическая защита текста определяется ключом и

алгоритмом шифрования, но не текстом; разные документы одной организации заверяются одной и той же печатью и т. п.

Результат *индикации* предписанных *технологических правил* обработки, передачи и хранения документа в течение его жизненного цикла с *допустимой* для сектора *достоверностью* должен вытекать из анализа атрибутов документа. Атрибуты, защищающие информацию документа, обусловлены не только и не столько информацией, сколько технологией ее отображения. Одна и та же технология может использоваться для документов с различным содержанием, равно как одна и та же информация может быть представлена разными технологиями в виде документа. В любом случае атрибуты и содержание конкретного документа должны быть, в некотором смысле, неотъемлемы друг от друга.

4.2. Мультипликативная парадигма защиты электронного обмена информацией

В ряде случаев в практике обеспечения информационной безопасности смешиваются детерминированные и вероятностные контексты того или иного события, в частности понятия угрозы и атаки. В хорошей в целом монографии [70], в частности, обосновано говорится:

Угроза безопасности вычислительной системе (ВС) — возможное воздействие, которое прямо или косвенно может нарушить состояние защищенности информации, содержащейся и обрабатывающейся в ВС.

Атака — реализация угрозы безопасности ВС.

Тем не менее, вывод, который делается в цитированных источниках, сомнителен: — «Цель защиты систем обработки информации — противодействие *угрозам* безопасности».

В идеале это, быть может, правильно. Но в реальности главная цель — отражение атак, борьба с угрозами вторична, хотя и не исключается. Угроза — *потенциальная*, и потому постоянно существующая опасность. Угрозы известны, т.е. детерминированы. Но далеко не всегда угроза реализуется в

виде атаки — атака есть событие *случайное*. *Всегда* существует *угроза* падения на компьютер тяжелого предмета, но редко осуществляется собственно падение предмета. Из наличия постоянной угрозы не следует, что корпус компьютера надо делать бронированным. Вероятностный подход к информационной безопасности выглядит достаточно перспективным.

Введем следующие определения и обозначения.

- $T = \{t_k, k = \overline{1,K}\}$ — конечное дискретное множество моментов времени t_k.
- $W = \{o_n, n = \overline{1,N}\}$ — конечное дискретное множество отдельных технологических операций (процессов) o_n информационного взаимодействия, где n — номер процесса.

Текущая *технология* $O(t_k)$ в момент *задана*, если известна последовательность нулей и единиц длины N, такая, что на n-м месте стоит 1, если в этот момент операция (процесс) o_n активизирована (выполняется), и стоит 0 — если нет.

Технология $O(T)$ задана, если для всякого момента $t_k, k = \overline{1,N}$, известна текущая технология $O(t_k)$.

В общем случае технологию $O(T)$ можно представить в виде матрицы O из нулей и единиц размера $K \times N$, элемент o_{kn} которой равен 1, если в момент времени t_k, $k=\overline{1,K}$, операция o_n, $n=\overline{1,N}$, активизирована, и равен нулю — если нет.

- $U = \{u_m, m = \overline{1,M}\}$ — конечное дискретное множество возможных угроз технологии $O(T)$, где m — номер угрозы.

Каждой угрозе u_m ставится в соответствие неотрицательное число, не превосходящее единицы, — вероятность реализации угрозы в виде атаки.

Допущение 1. Атаки a_m попарно независимы: реализация любой угрозы не влияет на реализацию остальных.

Строго говоря, допущение не совсем корректно. Во-первых, из попарной независимости событий иногда не вытекает их совместная

независимость. Во-вторых, если повреждающее воздействие намеренно, то обычно применяется пакет атак на ВС. Но это не столь существенно: на практике пространство попарно независимых, но взаимно зависимых в совокупности событий практически не встречается [71]; как правило, можно «укрупнить» пространство атак, рассматривая пакет атак как единую атаку.

Допущение 2. Длительность атаки существенно превосходит (машинное) время реализации технологии электронного обмена информацией.

Допущение не столь критично, как кажется на первый взгляд. Если атака произошла намеренно, то допущение выполняется почти всегда: атака реализуется в «человеческом» масштабе времени, а воздействие на технологию — в «электронном». Следует различать время *активизации* (реализации) технологии и время электронного взаимодействия. Обмениваться документами можно часами, но реализация обмена для каждого отдельного документа длится миллисекунды. Если атака случайная, например, сбой в процессе, то допущение только усиливает ее воздействие.

Из допущения 2 следует, что для каждого единичного акта документооборота условия можно считать фиксированными на момент начала взаимодействия. Тем самым, пространство атак можно считать постоянным в течение всего времени реализации технологии *конкретного* акта электронного взаимодействия и описать подмножеством реализованных угроз в любой момент времени t_k. В любой дискретный момент времени t_k пространство атак можно описать последовательностью нулей и единиц длины M, где на m-м месте стоит 1, если в этот момент атака a_m имеет место (угроза o_m активизирована), и стоит 0 — если нет.

- $r_m = 1 - s_m$ — вероятность реализации угрозы u_m в виде атаки a_m. (4.2.1)

Опираясь на допущение 1, на множестве угроз M строится вероятностное пространство атак, состоящее из 2^M элементов.

Технология $O(T)$, как показано выше, состоит из множества операций, поэтому, прежде чем оценивать характеристики безопасности технологии, рассмотрим таковые для отдельной операции.

Уточним понятия защищенности и безопасности объекта. Хотя эти понятия и связаны друг с другом, но это далеко не одно и то же.

Защищенность – характеристика объекта, определяющая его способность противостоять атакам.

Защищаются не от угрозы, защищаются от атаки. Понятие защищенности неизбежно связано с явной или неявной *конкретизацией* атаки. Если вероятность атаки отсутствует, то говорить о защищенности объекта бессмысленно. Защищенность человека со спасательным кругом выше человека без круга, если «человек за бортом» и подвергается атаке водной стихии, чем, если он делает ремонт в квартире.

Индексом защищенности r_{nm} операции o_n от атаки a_m (если известно, что атака a_m произошла) называется *условная* вероятность отражения атаки a_m при нападении на операцию o_n.

- $r_{nm} \hat{I} \{0,1\}$ — индекс защищенности операции (процесса) o_n от атаки a_m : $r_{nm} = 1$, если операция o_n защищена от атаки a_m (атака не влияет на операцию или отражается средствами защиты), и $r_{nm} = 0$, если операция o_n повреждается атакой a_m (атака успешна).

Безопасность – способность объекта сохранять свои номинальные параметры в заданных условиях окружающей среды.

Определение безопасности неизбежно требует *конкретизации* среды функционирования объекта. Если в среде атаки отсутствуют, то объект в безопасном состоянии, при этом не важно: защищенный он или нет.

Безопасностью p_n операции o_n называется *безусловная* вероятность сохранения операцией номинальных параметров (штатной реализации) в окружающей среде.

Утверждение 1. Для заданного выше пространства атак безопасность p_n операции o_n определяется из соотношения:

$$p_n = \prod_{m=1}^{M}[1 - r_m(1 - r_{nm})] = \prod_{m=1}^{M}(s_m + r_m r_{nm}) \qquad (4.2.2)$$

Доказательство. Если операция находится в безопасном состоянии, то для любой угрозы u_n имеет место: либо отсутствие реализации (атаки) — вероятность чего $s_m = 1 - r_m$, либо наличие реализации в виде атаки, но отражение последней — тогда вероятность равна $r_m r_{nm}$. В силу взаимной независимости атак вероятность их совместного осуществления равна произведению вероятностей каждого осуществления, откуда сразу следует (4.2.2). +

Если $p_n = 1$, то говорят, что операция *абсолютно безопасна*.

Следствие 1.1 Операция абсолютно безопасна, если индекс защищенности от любой из атак равен единице.

Для доказательства достаточно положить в (4.2.2) $r_{nm} = 1$, для любого m, тогда $p_n = 1$. +

Предложенный подход позволяет ввести обобщенную оценку защищенности операции o_n при неявном задании множества атак.

Обобщенным индексом защищенности d_n, или, просто, *защищенностью* d_n операции o_n называется *условная* вероятность (если известно, что атаки на операцию имеются) отражения всех атак при нападении на операцию.

Утверждение 2. Защищенность d_n операции o_n определяется из соотношения:

$$d_n = \frac{p_n - \prod_{m=1}^{M} s_m}{1 - \prod_{m=1}^{M} s_m} = \frac{\prod_{m=1}^{M}(s_m + r_m r_{nm}) - \prod_{m=1}^{M} s_m}{1 - \prod_{m=1}^{M} s_m} = 1 - \frac{1 - \prod_{m=1}^{M}(s_m + r_m r_{nm})}{1 - \prod_{m=1}^{M} s_m} \qquad (4.2.3)$$

Доказательство. Пусть d_n известно. Вероятность отсутствия атак на операцию o_n есть, учитывая их взаимную независимость, $\prod_{m=1}^{M} s_m$. Тогда вероятность наличия хотя бы одной атаки равна $1 - \prod_{m=1}^{M} s_m$. Безопасность p_n операции o_n находится по формуле полной вероятности в виде

$$p_n = \prod_{m=1}^{M} s_m + d_n(1 - \prod_{m=1}^{M} s_m) \qquad (4.2.4)$$

Приравнивая (4.2.2) и (4.2.4), сразу получим доказываемое соотношение (4.2.3) +

Предлагаемый критерий d_n защищенности операции o_n обобщает существующие подходы к оценке защищенности и удовлетворяет интуитивным представлениям о критерии защищенности. Опираясь на соотношение (4.2.4), можно установить справедливость следующих предложений.

Следствие 2.1. Если индекс защищенности r_{nm} операции o_n от любой атаки a_n равен единице, то защищенность d_n этой операции равна единице.

Доказательство.

$$\forall\, m = \overline{1,M},\ r_{nm} = 1: \qquad d_n = \frac{\prod_{m=1}^{M}(s_m + r_m) - \prod_{m=1}^{M} s_m}{1 - \prod_{m=1}^{M} s_m} = \frac{1 - \prod_{m=1}^{M} s_m}{1 - \prod_{m=1}^{M} s_m} = 1. + \qquad (4.2.5)$$

Следствие 2.2. Если индекс защищенности r_{nm} операции o_n от любой атаки a_m равен нулю, то и её защищенность d_n равна нулю.

Доказательство.

$$\forall\, m = \overline{1,M},\ r_{nm} = 0: \qquad d_n = \frac{\prod_{m=1}^{M} s_m - \prod_{m=1}^{M} s_m}{1 - \prod_{m=1}^{M} s_m} = 0. + \qquad (4.2.6)$$

Следствие 2.3. Если вероятность реализации угрозы u_M, от которой операция o_n не защищена, равна 1 (т. е. $r_M = 1$), то защищенность d_n этой операции равна нулю.

Доказательство.

$$\exists M,\ r_{nM} = 0,\ s_M = 1 - r_M = 0: \qquad d_n = \frac{r_{nM} r_M \prod_{m=1}^{M-1}(s_m + r_{nm} r_m) - s_M \prod_{m=1}^{M-1} s_m}{1 - s_M \prod_{m=1}^{M-1} s_m} = 0. + \qquad (4.2.7)$$

Следствие 2.4. Если при реализации операции o_n имеют место все атаки a_m: $m = \overline{1,M}$, то защищенность d_n этой операции равна произведению индексов защищенности r_{nm} от каждой из атак.

Доказательство.

$$\forall\ m = \overline{1,M},\ s_M = 1 - r_M = 0: \qquad d_n = \frac{\prod_{m=1}^{M}(s_m + r_{nm} r_m) - \prod_{m=1}^{M} s_m}{1 - \prod_{m=1}^{M} s_m} = \prod_{m=1}^{M} r_{nm}\ . + \qquad (4.2.8)$$

Следствие 2.5. Если вероятность отсутствия атак на операцию o_n близка к нулю, (т. е. $\prod_{m=1}^{M} s_m \approx 1$), то с погрешностью $O[(1 - p_n)\prod_{m=1}^{M} s_m]$ безопасность p_n этой операции равна ее защищенности d_n, т. е.

$$\prod_{m=1}^{M} s_m \approx 1: \qquad d_n = p_n + O[(1 - p_n)\prod_{m=1}^{M} s_m] \cong \prod_{m=1}^{M}(s_m + r_{nm} r_m)\,. \qquad (4.2.9)$$

Доказательство.

Для доказательства достаточно разложить соотношение (4.2.3) по степеням малости $\prod_{m=1}^{M} s_m$, учитывая, что $(1 - x)^{-1} = 1 + x + O(x^2)\,. +$

Условие $\prod_{m=1}^{M} s_m \approx 1$ характеризует окружение операции, в котором *точно* имеются атаки на операцию — *агрессивное окружение*. Следствие 2.5 можно переформулировать: — «В агрессивном окружении безопасность операции равна ее защищенности».

Рассмотрим теперь более общий случай — технологию $O\{*\}$: структурированную совокупность операций из подмножества $\{*\}$ множества N, $\{*\} \subseteq N = \{o_n : n = \overline{1,N}\}$.

Поскольку некоторые операции технологии o_n в компьютере могут выполняться одновременно, то предполагается структурированность, говорить об упорядоченности операций не совсем верно. Однако в машинах Тьюринга всегда существует эквивалентное представление любой технологии в виде строго упорядоченной *последовательности* отдельных операций из подмножества $\{*\}$ множества N. Теоретически это означает, что *технология не повреждена, если, и только если, не повреждены комплектующие ее операции*. В таком случае характеристики безопасности технологии должны выражаться аналогично рассмотренным для отдельных операций.

Индексом защищенности $r_{\{*\}m}$ технологии $O\{*\}$ от атаки a_m называется *условная* вероятность (если известно, что атака a_m произошла) отражения атаки a_m при нападении на технологию $\{*\}$.

Утверждение 3. *Индекс защищенности* $r_{\{*\}m}$ технологии $O\{*\}$ от атаки a_m равен произведению индексов защищенности каждой из операций, формирующих технологию $O\{*\}$,

$$r_{\{*\}m} = \prod_{o_n \in \{*\}} r_{nm} . \qquad (4.2.10)$$

Доказательство. Согласно допущению 2 можно пренебречь разновременностью операций технологии $O\{*\}$ и считать, что атака a_m наблюдается *в течение всего периода реализации* технологии, т.е. угрожает каждой из операций, образующих технологию. Влияние атаки a_m на каждую из операций o_n определяется индексом защищенности r_{nm}, где $o_n \in \{*\}$. Причём повреждение любой из операций подмножества $\{*\}$ необходимо влечет искажение результата: в *вероятностном* смысле операции соединены *последовательно*. Заметим, что только в вероятностном смысле, логическая

структура технологии может быть произвольной. Для безотказности последовательной цепи событий необходима безотказность каждого из событий. Отсюда сразу следует доказываемое. +

Безопасностью $p_{\{*\}}$ технологии $O\{*\}$ называется *безусловная* вероятность номинальных параметров (штатной реализации) технологии в окружающей среде.

Рассуждая, как и в утверждении 1, получим, учитывая (4.2.10),

$$p_{\{*\}} = \prod_{m=1}^{M}[1 - r_m(1 - r_{\{*\}m})] = \prod_{m=1}^{M}(s_m + r_m r_{\{*\}m}) \qquad (4.2.11)$$

Защищенностью $d_{\{*\}}$ технологии $O\{*\}$ называется *условная* вероятность (если известно, что атаки на технологию имеются) отражения атак при нападении на технологию. Аналогично соотношению (4.2.3), легко установить

$$d_{\{*\}} = \frac{p_{\{*\}} - \prod_{m=1}^{M} s_m}{1 - \prod_{m=1}^{M} s_m} = \frac{\prod_{m=1}^{M}(s_m + r_{\{*\}m} r_m) - \prod_{m=1}^{M} s_m}{1 - \prod_{m=1}^{M} s_m} \qquad (4.2.12)$$

Очевидно, что и следствия 2.1 – 2.5 могут быть почти дословно установлены и для случая анализа защищенности технологии $O\{*\}$. Из соображений компактности эти положения здесь не формулируются.

При анализе безопасности технологии информационного обмена выделяются две масштабные единицы времени.

Динамический период $\overline{m}$ — интервал $[t, t+m)$ технологической реализации *единичного* акта документооборота. Для динамического периода выполняется допущение 2 — его длительность m много меньше длительности q любой из атак множества A, $m << q$. Отсюда сразу следует постоянство в течение динамического периода как множества угроз U, так и множества атак : атака a_m входит в A с вероятностью r_m и не входит с вероятностью $s_m = 1 - r_m$, где вероятности r_m, s_m фиксируются на начало периода $r_m = r_m(t)$, $s_m = 1 - s_m(t)$.

Статический период $\bar{t}$ — промежуток времени t между последовательным обновлением электронной среды, восстанавливающим исходное состояние множества W технологических операций. Почти всегда $t \gg q \gg m$, например, период t между перезагрузкой системы в начале каждой рабочей смены. Период характеризуется *фиксированным* составом угроз U и *переменным* составом множества атак $A(t)$, $0 \le t \le t$, атака a_m генерируется в какой-то момент статического периода, длится некоторое время q и завершается. Наблюдается случайный процесс «гибели и размножения». Отношение суммарного времени длительности атак a_m к общей длине периода t равно, в первом приближении, вероятности r_m атаки a_m в динамическом периоде.

Легко видеть, что с математической точки зрения предложенный подход справедлив и для анализа информационной безопасности технологии взаимодействия в статическом периоде. Всегда можно в технологии $O\{*\}$ динамического периода в интервале $[t, t+m)$ положить $t=0$, $m=t$, и тогда рассуждения сводятся к предыдущему случаю. Однако исходные условия должны быть откорректированы с учетом качественного отличия промежутков времени m и t.

Во-первых, технология $O\{*\}$ в статическом периоде базируется на много более широком множестве операций, чем при единичном акте обмена электронной информацией.

Допущение 3. Технологическая база электронного взаимодействия *безизбыточна* — любая из технологических операций рано или поздно инициализируется хотя бы раз в течение периода взаимодействия.

Допущение означает, что анализ информационной безопасности исходит из наихудшего случая востребованности всех программно-аппаратных ресурсов ВС в период взаимодействия. Современное программное обеспечение настолько сложно, что конкретизация неиспользуемых ресурсов, как правило, невозможна, если период

взаимодействия достаточно длителен, например, рабочая смена. Во всяком случае, это задача не для рядового пользователя.

В течение рабочего дня используются разнообразные технологии, в общем случае применяются все операции o_n из располагаемого множества операций $W = \{o_n,\ n = \overline{1,N}\}$, т. е. надо говорить о технологии $O\{W\}$. Как и выше, различаются понятия защищенности и безопасности технологической базы. В соответствии с допущением 3 считается, что база формируется всем множеством $W = \{o_n, n = \overline{1,N}\}$ технологических операций (процессов) информационного взаимодействия, где n — номер процесса.

Поэтому индекс $r_{\{W\}m}$ защищенности технологии от атаки a_m должен в соответствии с (4.2.10) определяться по всему множеству $W = \{o_n, n = \overline{1,N}\}$

$$r_{\{W\}m} = \prod_{o_n \in \{W\}} r_{nm} \qquad (4.2.13)$$

Во-вторых, приемлемые для практических нужд критерии безопасности информационных технологий, применяемых в течение статического периода, обычно допускают только единичные нарушения отдельных актов электронного взаимодействия. При большом количестве нарушений дискредитируется весь период t. Вероятность $r_m(t) = 1 - s_m(t)$ атаки a_m в статическом периоде $\bar{t}$ существенно возрастает по сравнению с динамическим, что приводит при анализе статического периода к предпосылке агрессивной среды. Выполняются условия следствия 2.5, и почти всегда, особенно при повышенных требованиях к безопасности, справедливо положение: — «Безопасность $p_{\{W\}}(t)$ информационных технологий в статическом периоде взаимодействия $\bar{t}$ равна их защищенности $d_{\{W\}}(t)$ в течение периода t».

$$t \square m \qquad p_{\{W\}}(t) = \prod_{m=1}^{M} [1 - r_m(t)(1 - r_{\{W\}m})] = \prod_{m=1}^{M} [s_m(t) + r_m(t) r_{\{W\}m}] \cong d_{\{W\}}(t). \qquad (4.2.14)$$

Можно выделить два класса задач информационной безопасности.

Обеспечение защиты отдельных технологических операций (процессов) при их активизации. Так как активизация операции автоматически означает, что в это время протекает процесс преобразования собственно информации, то динамические задачи сводятся именно к защите информации. Например, защита от перехвата сигнала при обеспечении конфиденциальности информации.

Обеспечение защиты технологической базы в течение длительного периода функционирования ВС. В любой конкретный момент в ВС активизирована всегда очень малая, но не одна и та же, часть располагаемых операций. Решение статических задач неизбежно обусловлено наличием пассивной формы информации (хранением) в электронной среде существования, в том числе, «информации–технологии» (программных файлов). В таком случае, статические задачи заключаются в сохранении эталонного состава вычислительной среды (программных средств) и в обеспечении эталонного (санкционированного) доступа к этим средствам. Обратим внимание, что здесь не говорится о данных — любой доступ к данным (например, чтение файла) возможен, только если имеется доступ к соответствующим операциям (копировать, вывести на экран, читать и др.)

Соотношения (4.2.13), (4.2.14) характеризуют мультипликативность защитных свойств вычислительной системы. В соответствии с (4.2.13) для построения гарантированно защищенной вычислительной системы достаточно обеспечить защиту всех ее элементов от каждой из возможных атак на ВС. Тогда индекс защищенности $r_{\{N\}m}$ от любой атаки a_m равен единице, и согласно (4.2.14) безопасность и защищенность системы равна единице при любом распределении атак a_m. Свойство мультипликативности относится к наиболее общим закономерностям в среде безопасности, а именно: «степень безопасности системы определяется степенью безопасности ее самого «слабого» элемента» [72] или «итоговая прочность защищенного контура определяется его слабейшим звеном» [54].

Как показывает выражение (4.2.14), это условие достаточное, но не необходимое. Если вероятность атаки a_m низка, то высокий уровень безопасности может быть достигнут и без применения специальных средств защиты, что позволяет на практике существенно удешевить защиту ВС. Например, использовать механизмы, основанные на кодах аутентификации вместо асимметричной криптографии. Однако, предварительный анализ пространства угроз обязателен при решении проблем обеспечения информационной безопасности технологий электронного взаимодействия.

4.3. Доверенная вычислительная среда — ДВС. Резидентный компонент безопасности — РКБ

Разрабатываемая модель аппаратной защиты технологии электронного взаимодействия лежит в классе субъектно-объектных (СО) моделей и, развивая существующие СО-модели, направлена на более адекватный учет реальных условий электронного взаимодействия. В известных моделях, основные положения которых рассмотрены в гл. 1, накладываются чрезмерные ограничения на программно-аппаратный комплекс ВС. Даже проверка выполнения подобных ограничений в сложных корпоративных ВС крайне затруднительна на практике.

В главной своей части требования сводятся к обеспечению изолированности программной среды. Понятие изолированной программной среды (ИПС) введено в [59], где и дано ее формальное описание. Обобщая, можно сказать, что изолированная программная среда это совокупность (множество) программ, в которой:

- никакая активизированная программа не влияет на другую активизированную программу;
- никакая активизированная программа не влияет на данные, которые используются для создания (активизации) другой программы;
- каждая программа может использовать только те данные, которые ей разрешено использовать политикой безопасности;

- каждая программа может активизировать только те программы, целостность которых установлена и активизация которых ей разрешена политикой безопасности.

Постулируется, что изолированная программная среда должна поддерживать «любую разумную непротиворечивую политику безопасности». Если непротиворечивость политики безопасности еще можно установить, то можно ли точно трактовать термины «любая» и «разумная»?

Как наиболее современная, CO-модель [59] позволила выявить важнейший факт – для изолированности программной среды недостаточно контролировать доступ пользователя к данным, необходимо контролировать еще и доступ программ к данным, а также процесс порождения одними программами других на основе контролируемых данных. Изолированная программа (в терминологии CO-модели она еще называется корректной) не обязательно является корректной по отношению к преобразованиям данных. Так, программа вычисления хэш-функции сама по себе может быть корректной (изолированной), но применение ее к электронному документу является некорректным, хотя бы в силу того обстоятельства, что однонаправленное преобразование нарушает изоморфизм.

Ограниченность модели ИПС обусловлена также и тем, что она инвариантна к объекту, и в силу этого объекты в ней не различаются. Действительно, проверка изолированности необходимо означает перечислимость объектов, относящихся к программам и данным, что практически невыполнимо в программной среде современных вычислительных машин фон-неймановского типа. В универсальных машинах большинство программ и данных *неразличимы*: в разных вычислительных процессах и даже на разных этапах одного и того же процесса выполняют разные задачи.

Условие об отсутствии влияния данных на программы заведомо не выполняется в современных языках программирования, в которых

возможность создания объектно-ориентированных программ является одной из основных.

Для установления целостности объектов в СО-модели ИПС применяется термин «тождественность», понимаемый как «одинаковость в языке описания». Если же возможностей терминологии не хватает, то используется понятие «семантическая тождественность», очевидно неадекватное принципиальной точности электронной среды.

Но наиболее существенные ограничения СО-модели ИПС определяются принятыми в ней допущениями [59]: «генерация ИПС рассматривается в условиях неизменности конфигурации тех компонентов системы, которые активизируются до старта процедур контроля целостности объектов…» И далее: «Неизменность данных компонентов обеспечивается *внешними по отношению* к самой системе методами и средствами. При анализе или синтезе защитных механизмов свойства указанных компонентов являются априорно заданными». В то же время сами «методы и средства» не конкретизируются, хотя именно разработка подобных «внешних методов и средств» представляет одну из основных трудностей при обеспечении информационной безопасности. Фактически за пределами модели остается важнейшая в защите информации проблема эталона: в разделе 4.1 показано, что защита информации, будь то документ или технология, явно или неявно базируется на сравнении наблюдаемого результата с эталоном. Проблема в том, что решение принимается всегда в условиях только *частичной* известности одного из сравниваемых объектов — результата и эталона. К тому же и сам компаратор, производящий сравнение, подвержен атакам и может выдавать неверные заключения.

Отмеченные положения позволяют конкретизировать приоритетные направления усовершенствования модели ИПС с целью более адекватного отображения в СО-модели реальных условий электронного обмена информацией. Предлагаемая усовершенствованная субъектно-объектная модель защиты технологии электронного обмена информацией называется

далее как модель *доверенной вычислительной среды — модель ДВС*. Концептуальные отличия модели ДВС от модели ИПС приводятся ниже.

1. Требование неизменности программных средств в модели ИПС ослабляется до ограничения *целостности*.

Во-первых, неизменность есть, строго говоря, характеристика только цифрового отображения информации, здесь неизменность может быть установлена, например, побитным сравнением двух двоичных последовательностей. Понимая электронную среду существования как множество элементов, взаимодействующих на основе формальных правил обработки, хранения и передачи цифровой информации, надо учитывать, что сами эти элементы реализованы в объектах аналоговой среды. Любой аналоговый объект принципиально вариативен, его параметры не могут быть измерены абсолютно точно, к тому же они изменяются с течением времени.

Ранее установлено, что в электронной среде информация существует в двух формах: в пассивном состоянии (хранение на диске) — в аналоговой; в активном состоянии (передача и преобразование) — в цифровой. По сути вычислительных процессов обе эти формы тесно связаны и не могут существовать одна без другой. Неизменности не бывает в аналоговой среде, среде приблизительности, здесь постоянство устанавливается и обеспечивается всегда с *конечной*, пусть и достаточно высокой, точностью. Нельзя говорить о неизменности записи на диске, хотя бы потому, что ее физическое размещение меняется с течением времени. Но можно говорить о целостности, понимая, что отображение записи в виде процесса при считывании неизменно.

Во-вторых, составы активизированных в разных интервалах времени процессов различаются, хотя бы за счет изменения обрабатываемой информации. Тогда что же означает неизменность среды? Постоянство программных средств, как активизированных, так и хранящихся в памяти? А что тогда делать с файлами документов, состав которых принципиально

вариативен? И здесь понятие целостности кажется более предпочтительным по сравнению с неизменностью.

Под целостностью вычислительной среды понимается стабильность в течение рассматриваемого периода в требуемом диапазоне состава объектов и процессов, их взаимосвязей и параметров функционирования.

Какой состав, какие параметры и взаимосвязи и в течение какого периода — это определяется конкретной задачей исследования. Нельзя ограничиваться только файловой структурой при анализе особенностей защиты различных объектов ВС.

2. Замена требования неизменности ограничением целостности концептуально сказывается на задачах защиты информации. Неизменность — синоним фиксированности, и требование неизменности логично предполагает статическую модель явления. Кстати, рассмотренное в гл. 1 распространенное представление об электронном документе как об информации, *зафиксированной* на машинном носителе, по существу, есть статическая модель ЭлД. Целостность — следствие динамического характера информации в электронной среде, ее отображения как процесса, интерпретации технологии как информации.

Вычислительная среда меняется во времени, и задача защиты информации — обеспечение изменений в предусмотренном, штатном, режиме. Но тогда задача становится динамической, а динамический характер принципиально требует отслеживания изменений во времени. Если требуется отслеживать *целостность* среды, то надо знать ее *меняющиеся* во времени параметры, необходимо приходится «влезать» в среду, измерять, сравнивать ее параметры с эталоном. Для изолированной среды такое требование не является, вообще говоря, обязательным — достаточно никого «не пускать» в среду.

Следовательно, *доверенная программная среда принципиально предполагает наличие некоего «контролера», отслеживающего ее параметры, — компонента безопасности (КБ).*

3. А где должен находиться компонент безопасности, вне вычислительной среды или «внутри», являться одним из элементов среды? Если — «вне», то обязательно должен быть некий элемент, «разрешающий» такой контроль и, быть может, даже вмешательство в процесс функционирования среды при фиксации нежелательных режимов. И задача сводится к предыдущей. Наиболее очевидный ответ — компонент безопасности целесообразно встраивать в состав вычислительной системы, это должен быть «присутствующий — *resident*» объект. Исходя из этого требования, далее будем его называть *резидентный компонент безопасности* — РКБ.

С практических позиций, включение РКБ в состав вычислительной системы предоставляет широкие возможности для возложения на него и ряда дополнительных, помимо контроля, функций: оповещения, регулирования и управления процессами в вычислительной среде.

4. С одной стороны, РКБ предназначен для защиты электронной среды, а с другой — сам является элементом этой среды и, таким образом, сам нуждается в защите. Теоретически идеальная защита вычислительной среды недостижима, но практически это сводится к тому, что сам РКБ должен обладать намного более высоким индексом защищенности, нежели остальные элементы вычислительной среды.

Ранее установлено, что аппаратная реализация технологических операций, процедур, протоколов изначально обладает более высоким потенциалом защиты, чем программная. Поэтому при практической реализации РКБ должны превалировать аппаратные методы. Из этого, конечно, не следует, что такое направление повышения защищенности средства защиты единственно, что РКБ должны непременно реализовываться аппаратном виде. За все приходится платить — здесь теряется гибкость и адаптируемость. Возможны иные пути, в том числе, редуцирование вычислительных возможностей, например, РКБ с перестраиваемой

структурой. А в ряде случаев предпочтительнее чисто программная реализация, например, межсетевые экраны.

5. Понимая, что абсолютно надежных средств защиты не существует, и полагая, что злоумышленник в состоянии преодолеть защиту на любом этапе, разумно стремиться к получению реальных результатов, а не к бесплодным попыткам достичь идеальную цель — к созданию и поддержанию доверенной вычислительной среды, но не к обеспечению ее изолированности.

Фрагмент среды электронного взаимодействия, для которого установлена и поддерживается в течение заданного интервала времени целостность объектов и целостность взаимосвязей между ними, называется ***доверенной вычислительной средой — ДВС.***

6. Электронный документооборот в ВС основан на следующей взаимосвязи субъектов и объектов: оператор — за ПЭВМ в ЛВС — с ОС — используя ППО — и данные — формирует ЭлД — передаваемый в ВС — обрабатываемый в ВС — и хранимый в ВС — исполняемый в ВС.

Это означает, что применяемые РКБ должны участвовать в обеспечении информационной безопасности на следующих этапах реализации технологии электронного обмена данными (задачи 1—8):

1. Контроль целостности технического состава ПЭВМ и ЛВС.
2. Контроль целостности ОС.
3. Контроль целостности ППО и данных.
4. Распределение доступов и защита среды при доступе извне среды (межсетевые экраны, антивирус, и др.).
5. Контроль идентификации/аутентификации (ИА) пользователей.
6. Аутентификация документа при его создании.
7. Защита документа при его передаче (шифрование, ЭЦП и т.п).
8. Аутентификация документа при обработке, хранении и исполнении документа.

Такое разделение задач не противоречат требованиям нормативных документов Гостехкомиссии, а является их необходимым дополнением, тем более что изложенные в [73] требования характеризуют каждый класс только минимальной совокупностью требований по защите.

4.4. Концептуальные особенности резидентного компонента безопасности

4.4.1. Автономность и независимость РКБ от защищаемой среды

Из общесистемных понятий вытекает, и многовековой опыт это подтверждает, что наилучшие результаты достигаются, когда средства защиты функционируют максимально автономно от защищаемого объекта. Покажем, что в случае взаимозависимости качество защиты ухудшается.

Пусть функционирование средств обеспечения и состояние защищаемого объекта *полностью* взаимозависимы. Если вероятность отсутствия атаки a_m равна единице, $s_m = 1 - r_m = 1$, то согласно соотношению (4.2.11) мультипликативной модели безопасность $\pi_{\{*\}}$ технологии $O\{*\}$ равна единице при любом индексе $\rho_{\{*\}}$ ее защищенности. В этом случае технология реализуется штатно, соответственно и средства защиты функционируют нормально. Поскольку атак нет, то и защита не нужна, разве что защищаться от угроз. Порочность подобной постановки вопроса уже была показана (раздел 4.2). Если угроза реализуется в виде атаки и воздействует на защищаемую технологию, то, в силу взаимозависимости, парализуются и средства защиты. И опять защита оказывается ненужной — как раз в нужный момент она «отключается».

При частичной взаимозависимости рассуждения аналогичны, результат меняется количественно: вместо «защита бесполезна» — «защита в ряде случаев бесполезна». Конечно, на практике взаимозависимость исключить невозможно, абсолютная автономность недостижима — защита и объект связаны всегда, хотя бы потому, что *данное* средство защищает именно

данный объект. В той или иной степени защита обеспечивается и при общем базисе. Очевидно, по этой причине в сфере информационной безопасности широко распространено представление, что полноценная защита программной среды может быть обеспечена *целиком* программными методами: межсетевые экраны, антивирусные программы и т. п. Практическое удобство и полезность таких мероприятий бесспорна [74]. Тем не менее, стремиться надо к максимальной автономности, независимости средств защиты от защищаемого объекта. Поскольку защита неминуемо связана с индикацией состояния защищаемого объекта, то отсюда автоматически следует и общеизвестный принцип независимости средств контроля от контролируемого объекта. В реальной жизни это именно так. Центральный банк страны, контролирующий и защищающий денежную систему государства, должен быть отделен от исполнительной власти, распоряжающейся финансами. Налоговые органы действуют независимо от налогоплательщика.

С системных позиций, ориентация на защиту фрагмента электронной среды на базе методов и механизмов *того же самого* фрагмента не имеет достаточной перспективы. Это обусловлено не только тем, что при цифровом отображении ресурсы защиты информации много ниже, чем при использовании аналоговых методов. В том числе, и технологии — как информации о процессах обработки. Это количественный эффект. Важнее другая, качественная, системная причина: *высокая достоверность фрагмента среды детерминированных (точных) процессов принципиально не может быть обеспечена без выхода за рамки этого фрагмента*. Непрекращающаяся борьба с вирусами, червями, закладками подтверждает тезис.

Защита любого процесса базируется на явном или неявном сравнении результата обработки данным процессом известного тестового сигнала с априорно известным эталоном. Очевидно, что и компаратор, сравнивающий результат с эталоном, и сам эталон не должны зависеть от тестируемого

процесса, должны быть инвариантными относительно него. Но если, например, защищается процесс загрузки доверенной вычислительной среды, то средствами только загружаемого ПО обеспечить такую независимость невозможно. Компаратор будет работать на базе той же самой операционной среды, достоверность которой он устанавливает и, значит, будет зависим от среды.

Можно в загружаемое ПО включить программу, блокирующую измерение фактических результатов и подставляющую требуемое эталонное значение. Так как среда детерминированная, то подобная подстановка априорно вычислима и, следовательно, реализуема. Рассуждения не меняются, если тестируется некий вторичный процесс: подстановка может быть выполнена на предыдущих этапах. По существу, на качественном уровне подтверждается результат предыдущего раздела о необходимости некоторой начальной неизменяемой процедуры, эталона, выполняющего функцию точки опоры для следующих этапов.

Результат принципиально не меняется от того, как конкретно организуется сравнение результата с эталоном: на входе, выходе, «посередине». Механизмы защиты вторичны, диктуются конкретными условиями: можно, например, проверять исходные компоненты, и тогда продукт будет соответствовать требованиям, а можно контролировать готовый продукт, и это означает, что ингредиенты качественные. Что также следует из анализа проблем размещения РКБ, вводимые резидентные компоненты безопасности выполняют, по существу, функции хранения и сравнения эталона с фактическим результатом.

Резидентный компонент безопасности необходимо должен быть максимально автономен относительно программной среды, безопасность которой он должен обеспечивать.

4.4.2. Примитивность резидентного компонента безопасности

В разделе 4.3 было установлено, что РКБ должен *входить* в состав ВС, безопасность которой он обеспечивает. На первый взгляд приходим к противоречию, однако, это кажущийся парадокс. Входить в состав ВС и быть автономным относительно программной среды возможно: вычислительная система — это не только программные средства, это и аппаратная реализация, и интерфейсы, и стандарты взаимодействия, и др. Действительно, РКБ должен быть *совместим* с ВС, иметь возможность физически *входить* в состав системы. Одновременно он должен быть *независим* от вычислительной системы, т. е. *являться специализированным компьютером* с собственной операционной средой, памятью и прочими атрибутами фон-неймановской машины.

Теоретически возможно в качестве РКБ применить другой компьютер, если бы удалось обеспечить более высокий уровень его защищенности, чем у защищаемого компьютера. Эти задачи эквивалентны, если сопоставимы компьютеры — так что такое направление бесперспективно. РКБ как вычислительное устройство должно существенно отличаться от защищаемой среды, иметь много меньше уязвимостей. На практике почти всегда много проще не предоставлять конкретных возможностей для атаки, чем защититься от нее. В отличие от защищаемой универсальной электронной среды, компонент безопасности необходимо должен быть *узко специализированным*, примитивным компьютером.

Здесь выделяется только доминирующая характеристика компонента безопасности, логично вытекающая из его функциональной роли эталона, ведь эталон — это всегда неизменность, константа. И с указанных позиций аппаратная реализация РКБ выглядит более перспективной, нежели программная.

Итак, РКБ должен представлять собой вычислительную машину, причем надо стремиться, чтобы возможности его были *максимально*

ограничены. Универсальная машина Тьюринга основана на четырех элементарных операциях: сдвинуть ячейку влево, сдвинуть ячейку вправо, заменить символ в ячейке, остановиться. Необходимый и достаточный набор элементарных операций для работы ЭВМ в любом случае должен состоять из четырех операций, таких, что ни одна из этих операций не может быть выражена через композицию остальных. Так как две сложные процедуры «читать, адрес где» и «писать, адрес куда» базируются, по существу, на четырех независимых в совокупности процессах, то они исчерпывающе описывают основанное на их использовании вычислительное устройство.

Отметим одно важное обстоятельство, на которое обычно не обращают внимание. Машина Тьюринга принципиально является машиной последовательной, так что, теоретически, совсем не требуется, чтобы все четыре операции существовали одновременно. Если *априорно* известно, что некоторая операция будет выполняться n тактов подряд, то остальные операции в это время не нужны. Строго говоря, переключаемое устройство, которое в один период времени (в человеческом масштабе) «пишет», а в другой — «читает», есть, в долговременном смысле, полноценная машина Тьюринга. А значит, и это принципиально, с этим устройством *практически возможно* сопряжение и взаимодействие стандартных компьютеров.

Ну а что может быть в рассматриваемом контексте ограниченнее, чем *компьютер* в долговременном смысле, *который не является компьютером* в любой краткосрочный период. Сколь эффективно сужаются возможности негативного воздействия на работу такого вычислительного устройства: чем меньше возможностей — тем лучше защита.

Принцип примитивности, ограниченности свойств РКБ как вычислительного устройства позволяет конкретизировать его сущность и статус в рамках вычислительной системы. Логично возложить подавляющее большинство вспомогательных функций сопряжения и взаимодействия РКБ с ВС на устройства системы, оставив на долю РКБ только «руководство». В цифровой детерминированной среде взаимоотношения, права и обязанности

«руководителя и подчиненных» задаются *абсолютно* точно, однозначно. Поэтому необходимо выполнение двух требований:

- РКБ как «руководитель» должен «знать» в процессе функционирования эталонный результат технологических процессов — хранить эталон и позволять его варьировать *извне* при изменении требований сектора действенности к технологии информационного взаимодействия.
- Устройства ВС, «подчиненные РКБ», должны информироваться о требованиях РКБ в процессе выполнения соответствующих технологических процедур и операций.

Выполнение требования минимальной конфигурации РКБ как вычислительного устройства возможно в таком случае только если интерпретировать его, пусть это очень схематично, как долговременное запоминающее устройство. Действительно, тем или иным способом в РКБ извне записывается эталон, а развитые исполнительные устройства защищаемой системы считывают необходимые инструкции из РКБ.

Другое дело, что реализация этого, вообще говоря, достаточно очевидного принципа на практике далеко нетривиальна. Как обеспечить предельно санкционированный доступ к записи в РКБ? Как оперативно корректировать РКБ, учитывая, что состав программной среды постоянно меняется? И при этом сохранять неизменность? Как исключить действия исполнительных устройств ВС «в обход» РКБ, иначе — какие магистральные направления функционирования электронной среды должны «перекрываться» компонентом безопасности? Как обеспечить отсутствие искажений между эталоном и результатом, который доходит до исполнительных устройств? Считывающее устройство может, в принципе, внести «свои» корректировки.

Но все это вопросы вторичные, они будут рассмотрены ниже. С теоретических позиций ситуация ясна — резидентный компонент безопасности по своей функциональной сущности есть всего лишь запоминающее устройство.

4.4.3. Перестраиваемость резидентного компонента безопасности

Установленные в разделе 4.3 задачи безопасности (1—8) электронного обмена данными, в решении которых должен участвовать РКБ, можно разделить на две группы, соответствующие двум основным этапам работы вычислительной системы:

- этап формирования политики безопасности — *режим управления*;
- этап электронного обмена информацией — *пользовательский режим*.

Предметной областью задач первой группы (1—4, см. разд. 4.3) является среда существования документа, целостность и санкционированный доступ к которой должен обеспечиваться средствами защиты — *задачи целостности среды*. Здесь не существенен сам непосредственный носитель информации, собственно электронный документ. Во временном аспекте можно говорить об *этапе управления* средой или об этапе формирования политики безопасности. Считается, что описание политики безопасности, согласно которой функционирует ВС, зафиксировано в некоторой базе данных в виде правил разграничения доступа дискреционного механизма, меток конфиденциальности, мандатного механизма и т. д.

Задачи второй группы (5—8, см. разд. 4.3) характерны для *пользовательского режима* работы ВС — *задачи аутентификации объектов и субъектов*. В отличие от первой группы здесь приходится иметь дело с конкретными пользователями и конкретной информацией, конкретному сообщению придается статус документа. Основное содержание — решение проблем аутентификации субъектов, взаимодействующих с данным документом, санкционирование доступа к ЭлД. В том числе аутентификация субъектов, формирующих и применяющих данный ЭлД, а также имеющих доступ к документу в процессе документооборота. Специфика групп задач обусловлена *качественно разными* объектами защиты — среда и документ,

и, соответственно, должна отражаться в требованиях к РКБ, участвующих в их решении.

В таком случае, при обосновании архитектуры РКБ можно ограничиться изучением только двух принципиально отличающихся функциональных возможностей: чтение — R (*read*); запись — W (*write*) (адрес подразумевается и опущен для компактности). Точно такой же результат следует и из предыдущего раздела, где обсуждалась минимальная конфигурация РКБ: извне в РКБ *записывается* эталон, устройства ВС *считывают* из РКБ требуемый результат. На практике, конечно, потребуется целый ряд дополнительных требований к РКБ, обеспечивающих его сопряжение с ВС, совместимость и т. п. Тем не менее, в самом общем плане можно утверждать, что для функционирования РКБ достаточно реализации этих двух операций, причем адрес должен пониматься по умолчанию.

В *режиме управления* назначение РКБ — обеспечение легального формирования выбранной системным администратором политики безопасности. Для этого требуется внесение соответствующих изменений (записей) в базу данных компонента безопасности. Следовательно, для применимости РКБ на этапе управления ВС компонент необходимо должен обладать свойством «*записать*, *W*». С математических позиций, «стереть» запись эквивалентно — «записать»: например, одни «нули». Поэтому можно обойтись без операции чтения, не заменять записи, но записать всю базу полностью. Таким образом, в режиме управления наличие операции W не только необходимое, но и *достаточное* условие выполнения РКБ своего назначения.

В *пользовательском режиме* назначение РКБ — контроль соответствия доступа пользователей к интересующим их объектам вычислительной системы сформированной политике безопасности. Доступ либо разрешается, либо запрещается в соответствии с информацией из базы данных РКБ, содержащей правила функционирования ВС. Следовательно, для применимости РКБ в пользовательском режиме ВС компонент безопасности

необходимо должен обладать возможностью *чтения* R. В принципе, это и *достаточное* условие для реализации пользовательского режима работы РКБ.

Итак, для работы во всех режимах ВС достаточно, чтобы РКБ обладал свойствами R, W, что, согласно предыдущему разделу, означает, что РКБ будет полноценной машиной Тьюринга. Но тогда РКБ одновременно обладает этими свойствами и задача защиты ВС необходимо сводится к почти равноценной задаче защиты РКБ-компьютера. Легко привести пример разрушающего программного воздействия (РПВ), если РКБ одновременно обладает свойствами R, W. Если злоумышленник является легальным пользователем ВС, то, используя функциональные возможности РКБ, он может сначала выяснить свои права доступа к интересующему его объекту (с помощью процесса R), а затем заменить свои права на интересующие (с помощью процесса W).

Суммируя приведенные доводы, выделим следующие положения:

- для обеспечения защиты ВС резидентный компонент безопасности необходимо должен быть машиной Тьюринга;
- если РКБ в каждый момент времени может выполнять любую из тьюринговых операций, то построенные на такой базе механизмы защиты потенциально уязвимы;
- в цикле функционирования ВС можно выделить два непересекающихся режима — режим управления и пользовательский режим;
- для каждого из режимов достаточно функционирование РКБ с редуцированным множеством операций: в режиме управления W — запись, адрес; в пользовательском режиме R — чтение, адрес;
- РКБ с редуцированным множеством операций, как установлено в предыдущем разделе, имеет потенциально высокую защищенность.

Но тогда напрашивается следующее предложение — *РКБ не должен быть машиной Тьюринга в краткосрочном периоде, но должен являться таковой в долгосрочном*. Резидентный компонент безопасности должен

иметь перестраиваемую архитектуру, в каждый момент времени обладать редуцированным набором вычислительных операций: в режиме управления W — запись, адрес; в пользовательском режиме R — чтение, адрес. Это позволило бы сочетать отмеченные выше несовместимые требования.

Возникает вопрос, а кто (что) должен выдавать команду на перестройку РКБ? Вариант, что такой сигнал должен исходить от ВС, порочен в принципе. Согласно теореме о программировании последовательной композиции тьюринговых программ [13] всегда может быть построена программа T, которая будет реализовывать рассмотренный выше механизм РПВ. Остается единственная возможность — *перестройка архитектуры РКБ должна осуществляться извне, защищенным воздействием уполномоченного лица*.

4.5. Модели размещения резидентного компонента безопасности

4.5.1. Исходные предпосылки

Целостность вычислительной системы — технического состава, операционной системы (ОС), прикладного программного обеспечения (ППО) и данных — необходимое условие безопасности обмена электронной информацией. При условии целостности технического состава ВС следующим рубежом защиты является обеспечение и поддержание (защита от несанкционированной доступа — НСД) целостности программной среды. Исходным является естественное допущение, что в ПЗУ (BIOS) и операционной среде (в том числе и в сетевом ПО) отсутствуют *специально* интегрированные в них возможности НСД — т. е. система проверена, или сертифицирована.

Пусть пользователь работает с программой, в которой также исключено наличие каких-либо скрытых возможностей (проверенные программы). Потенциально злоумышленные действия могут быть такими:

- Проверенные программы будут использованы на другой ПЭВМ с другим BIOS и в этих условиях использоваться некорректно.
- Проверенные программы будут использованы в аналогичной, но не проверенной операционной среде, в которой они также могут использоваться некорректно.
- Проверенные программы используются на проверенной ПЭВМ и в проверенной операционной среде, но запускаются еще и не проверенные программы, потенциально несущие в себе возможности НСД.

Указанные события и, соответственно, НСД в ВС практически невозможны, если выполняются следующие условия.

У1 — на ПЭВМ с проверенным BIOS установлена проверенная операционная среда.

У2 — достоверно установлена неизменность DOS и BIOS для данного сеанса работы.

У3 — кроме проверенных программ в данной программно-аппаратной среде не запускалось и не запускается никаких иных программ, проверенные программы перед запуском контролируются на целостность.

У4 — исключен запуск проверенных программ в какой-либо иной ситуации, т. е. вне проверенной среды.

У5 — условия У1—У4 выполняются в любой момент времени для всех пользователей, аутентифицированных защитным механизмом.

В таком случае программная среда является доверенной — ДВС.

Обеспечение ДВС существенно ослабляет требования к базовому ПО, поскольку контролируется активизация процессов через операционную среду, целостность исполняемых модулей перед их запуском и разрешается инициирование процесса только при одновременном выполнении двух условий: принадлежности к разрешенным и неизменности. В таком случае от базового ПО требуется только:

- невозможность запуска программ помимо контролируемых ДВС событий;

- отсутствие в базовом ПО возможностей влиять на среду функционирования уже запущенных программ (фактически это требование невозможности редактирования оперативной памяти).

Все прочие действия, являющиеся нарушением Условий 1—3, в оставшейся их части будут выявляться и блокироваться. Таким образом, ДВС существенно снижает требования к ПО в части наличия скрытых возможностей.

Основным элементом поддержания доверенности среды является контроль целостности. Но контроль целостности необходимо сопряжен с чтением данных (по секторам, по файлам и т. д.), т. е. вмешательством в программную среду. Возможна ситуация, когда внедренное в систему разрушающее программное воздействие (РПВ) в процессе чтения будет навязывать вместо одного сектора другой или редактировать непосредственно буфер памяти. С другой стороны, даже контроль самого BIOS может происходить «под наблюдением» какой-либо дополнительной программы («теневой BIOS») и не показать его изменения. Аналогичные эффекты могут возникать и при обработке файла. Внедренное в систему РПВ может влиять на процесс чтения-записи данных на уровне файлов или на уровне секторов и предъявлять системе контроля некоторые другие вместо реально существующих данных. Этот механизм неоднократно реализовывался в STELS-вирусах.

Тем не менее, очевидно, что если программный модуль, обслуживающий процесс чтения данных, не содержал РПВ и целостность его зафиксирована, то при последующей неизменности этого программного модуля чтение с его использованием будет чтением реальных данных. Данный принцип предлагается реализовать с помощью следующего механизма ступенчатого контроля для создания ДВС.

При включении питания происходит тестирование ОП, инициализация таблицы прерываний и поиск расширений BIOS. При их наличии управление передается на них. После отработки расширений BIOS в память считывается

первый сектор дискеты или винчестера (загрузчик) и управление передается на него, код загрузчика считывает драйверы DOS, далее выполняются файлы конфигурации, подгружается командный интерпретатор и выполняется файл автозапуска. Тем самым при реализации ДВС предварительно фиксируется неизменность программ в основном и расширенных BIOS, далее, используя функцию чтения в BIOS (для DOS int13h), читаются программы обслуживания чтения (драйверы DOS), рассматриваемые как последовательность секторов, и фиксируется их целостность. Затем, используя уже файловые операции, читаются необходимые для контроля исполняемые модули (командный интерпретатор, драйверы дополнительных устройств, .EXE и .COM — модули и т. д.).

Очевидно, что при запуске ДВС контроль целостности должен выполняться таким же образом и в той же последовательности. Процесс аутентификации необходимо проводить в одном из расширений BIOS (чтобы минимизировать число ранее запущенных программ), а контроль запуска программ включать уже после загрузки DOS (иначе DOS определяет эту функцию на себя). При реализации ДВС на нее должна быть возложена функция контроля за запуском программ и контроля целостности.

Первый шаг алгоритма ступенчатого контроля для создания ДВС должен базироваться на применении некоторой неизменяемой (немодифицируемой) процедуры, выполняющей роль «твердой» точки опоры для следующих этапов. Не любой контроллер в состоянии обеспечить защитные функции: необходим достаточный ресурс постоянства самого контроллера для выполнения пошагового алгоритма контроля целостности и формирования ДВС. Предпочтительнее аппаратная реализация алгоритмических процедур.

В общем случае вычислительную систему можно рассматривать как некоторое множество элементарных (базисных) операций, под которыми в зависимости от конкретной задачи можно понимать отдельные операции, алгоритмы, процессы, процедуры, протоколы. Детализация здесь

несущественна. В первом приближении множество элементарных процессов — это все файлы, хранящиеся в устройствах долговременной памяти компьютера, будь то оперативная память, BIOS, кэш и т. д. Тогда используемую технологию информационного обмена можно интерпретировать как некоторую выборку с возвращением из базисного множества операций. Выбор с возвращением означает, что ряд элементарных операций (например, копирование или чтение) может неоднократно использоваться в составе данной технологии. Обратим внимание, что управляющую программу, т. е. алгоритм технологии, можно также рассматривать как элементарную операцию.

Очевидно следующее положение: «для целостности вычислительной системы необходимо и достаточно, чтобы целостной являлась любая технология, сформированная на базисном множестве элементарных операций». Целостность (только) элементарных операций необходима, но не достаточна: и на основе «доброкачественных» операций может быть сформирована некорректная технология. Пример вирусов хорошо иллюстрирует это положение. Строго говоря, установление целостности ВС необходимо требует установления целостности (корректности) *любой* логически непротиворечивой допустимой последовательности элементарных операций.

Известно, что число различных n-выборок (длиной n операций) с возвращением из m различных элементов равно m^n. При сколько-нибудь больших m и n абсолютное установление целостности системы практически невозможно, тестирование потребует огромного времени. Хотя логически реализуема лишь очень малая часть возможных выборок операций, но все равно очевидно, что лобовое решение задачи установления абсолютной целостности ВС бесперспективно. Очевидный путь уменьшения размерности — переход к более крупным масштабным единицам: сокращается как m, так и n. В этом случае вместо исходных элементарных операций рассматриваются структурированные объекты: процессы как организованная

совокупность операций, процедуры — детерминированная последовательность процессов, протоколы и т. д.

Но здесь возникает новая трудность — теряется доступ к отдельным элементарным операциям, и о целостности каждой из них приходится судить по кумулятивному результату. Не удается непосредственно проверить выполнение даже необходимого условия целостности ВС — целостность каждой операции. Кстати, это типичный случай. Почти всегда установление целостности отдельной операции физически осуществимо только при условии ее включения в некоторый более сложно организованный программный продукт. Встает задача установления целостности компонентов процесса на основе изучения процесса в целом.

Наиболее распространенными архитектурами организации вычислительных процедур являются линейная (последовательная) и древовидная (иерархическая). Поэтому ниже свойства таких архитектур анализируются специально.

4.5.2. Размещение резидентного компонента безопасности при обеспечении целостности технологий с линейной архитектурой

Наиболее важен начальный этап — от включения системы до активизации механизмов поддержки ДВС. В силу мультипликативности защитных свойств оставлять этот этап без защиты нельзя, и простого декларирования его свойств на практике недостаточно. Хотя модель доверенной вычислительной среды является развитием СО-модели изолированной программной среды, но она позволяет установить ряд новых положений, связанных с конкретной аппаратной реализацией РКБ, реализующих функции защиты доверенности среды.

Система имеет линейную архитектуру (линейная система), если множество объектов строго упорядочено — всякому объекту, за исключением начального, предшествует один и только один объект. Иначе, любой процесс технологии инициируется одним и только одним процессом.

- $O = \{o_i, i = \overline{1,N}\}$ — система из N взаимосвязанных объектов o_i (технология O, состоящая из N процессов o_i).

Система с линейной архитектурой может быть отображена в виде последовательности объектов o_i, начинающейся с объекта o_1 и заканчивающейся объектом o_N .

Определение 1. Линейная система является целостной, если установлена целостность каждого из ее объектов $o_i \in O$, $i = \overline{1,N}$.

Определение 2. Связь между любой парой объектов (o_i, o_{i+1}) при проверке целостности линейной системы описывается (n_i+1)-местной функцией проверки целостности объекта:

$f_i = f_i(o_i) = f_i(o_i, p_{i1}, p_{i2}, \ldots, p_{in_i}) = o_{i+1}, \quad i = \overline{1,N-1}$, где $p_{i1}, p_{i2}, \ldots, p_{in_i}$ — параметры объекта o_{i+1}. Функция f_i, $i = \overline{1,N-1}$, устанавливает целостность объекта o_{i+1}, если целостность объекта o_i зафиксирована. При этом функции $f_i(o_i) = o_{i+1}$, $i = \overline{1,N-1}$, являются функциями следования согласно [8].

Утверждение 4 (*об установлении целостности линейной системы*): целостность линейной системы установлена тогда и только тогда, когда установлена целостность объекта o_N.

Доказательство. Пусть система целостна, тогда по определению 1 установлена целостность всех объектов системы $o_i \in O$, $i = \overline{1,N}$. Следовательно, установлена целостность объекта o_N.

Пусть установлена целостность объекта o_N, т. е. известно значение функции проверки целостности $f_{N-1} = f_{N-1}(o_{N-1}, p_{N-1,1}, p_{N-1,2}, \ldots, p_{N-1,n_{N-1}}) = o_N$. Функция f_{N-1} определена только в том случае, когда установлена целостность объекта o_{N-1}. Рассуждая по индукции, придем к выводу, что из целостности объекта o_2 следует, что целостность объекта o_1 зафиксирована. Тем самым, зафиксирована целостность всех объектов системы $o_i \in O$, $i = \overline{1,N}$, и по определению 1 система целостная.

Таким образом, задача установления целостности линейной системы эквивалентна задаче установления целостности объекта o_N.

Пусть подмножество $M \subset O$ есть множество объектов системы, целостность которых установлена.

Определение 3. Множество M разрешимо, если существует алгоритм A_M, который по любому объекту o_i дает ответ, принадлежит o_i множеству M или не принадлежит.

Определение 3.* Множество M разрешимо, если оно обладает вычислимой всюду определенной (общерекурсивной) функцией $\square_M$, такой, что

$$c_M(o_i) = \begin{cases} 1, \text{ если } o_i \in M \\ 0, \text{ если } o_i \notin M \end{cases}. \qquad (4.5.1)$$

Определение 4. Множество M называется перечислимым, если оно является областью значений некоторой общерекурсивной функции, т.е. существует общерекурсивная функция $\Psi_M(x)$ такая, что $o_i \in M$, если и только если для некоторого $x \in N$ $o_i = \Psi_M(x)$. Функция $\Psi_M(x)$ называется перечисляющей для множества M. Из [75] известно

утверждение 5 **(***о разрешимости***)**. Множество M разрешимо, если и только если M и $\overline{M}$ перечислимы.

Определение 2.* Линейная система является целостной, если M — разрешимое множество и M совпадает с O, $M = O$.

Теперь может быть сформулировано

утверждение 6 (*об использовании резидентного компонента безопасности — РКБ*). Задача контроля целостности системы разрешима только при использовании специализированного аппаратного резидентного компонента безопасности (РКБ).

Доказательство. 1. Покажем, что без дополнительного компонента построение системы с установлением целостности невозможно.

Построим перечисляющую функцию для множества *M*. Она должна быть общерекурсивной, т. е. всюду определенной на *O* частично-рекурсивной функцией.

Определим функцию $\Psi_M(x)$ следующим образом:

$$\Psi_M(i) = o_i \,. \qquad (4.5.2)$$

Тогда ее можно представить через функции проверки целостности объектов f_i (См. Опред. 2). Для этого определим семейство операторов суперпозиции $\left\{ S^{n_i+1}_{n_{i+1}+1} \right\}$:

$$S^{n_i+1}_{n_{i+1}+1}(f_{i+1}, f_i) = f_{i+1}(o_i, f_i(o_i)). \qquad (4.5.3)$$

В этом случае перечисляющая функция примет вид: $y_M(i) = S^{n_i+1}_{n_{i+1}+1}(f_{i+1}, f_i)$.

При этом $\Psi_M(i)$ является частично-рекурсивной функцией, так как построена из функций f_i, которые являются элементарными как функции следования [75], путем последовательного к ним применения операторов суперпозиции $S^{n_i+1}_{n_{i+1}+1}$.

Однако $\Psi_M(i)$ не является всюду определенной, т.к. значение функции f_1 в точке o_1 не определено. Это объясняется тем, что не определена (согласно определению 2) связь f_0, которая устанавливала бы целостность объекта o_1. Причиной неопределенности функции f_0 является отсутствие объекта, который являлся бы областью определения функции f_0 и целостность которого была бы зафиксирована.

Следовательно, нельзя построить перечисляющую функцию множества *M* и множество *M* не является перечислимым.

Согласно теореме о разрешимости, множество *M* не является разрешимым, и, по определению 2*, система не является целостной.

2. Покажем, что при использовании РКБ построение целостной АС возможно.

Добавим в систему элемент o_0, целостность которого достоверно определена. Рассмотрим систему с множеством объектов $O^0 = O \mathbf{U} \{o_0\}$.

Определим связь f_0, устанавливающую целостность объекта o_1: $f_0(o_0) = f_0(o_0, p_{11}, \mathbf{K}, p_{1n_1}) = o_1$.

Тогда перечисляющая функция $\Psi_M(i)$ множества M будет задана согласно (4.5.2) следующим образом:

$$\begin{cases} y_M(0) = f_0(o_0) = o_1 \\ y_M(i) = S^{n_i+1}_{n_{i+1}+1}(f_{i+1}, \ f_i) = o_{i+1} \end{cases},$$

т. е. функция является частично-рекурсивной и определена на всем множестве O. Следовательно множество M – перечислимо.

Определим $\overline{M} = O^0 \setminus M = \{o_0\}$. Перечисляющая функция $y_{\overline{M}}$ для множества $\overline{M}$ может быть определена как функция аутентификации для объекта o_0.

$$\begin{cases} \psi_{\overline{M}}(0) = o_0, \quad \text{т.е.} \quad o_0 \in \overline{M} \\ \psi_{\overline{M}}(i) = o_i, \quad \{o_i\}_{i=1}^{N} = O, \ \text{т.е.} \ o_i \notin \overline{M} \end{cases} \qquad (4.5.4)$$

В этом случае $y_{\overline{M}}$ является всюду определенной, вычислимой, т. е. общерекурсивной функцией, следовательно, множество $\overline{M}$ является перечислимым.

Тогда, по теореме о разрешимости, M есть разрешимое множество, следовательно, в силу определения 1, целостность системы может быть установлена.

Из доказанного утверждения об использовании РКБ следует:

Следствие 6.1: установление целостности возможно только при расширении АС специализированным резидентным компонентом безопасности (РКБ).

Следствие 6.2: установление целостности АС невозможно только за счет программных средств без использования резидентного компонента безопасности (РКБ).

Рассмотрим теперь вопрос о размещении компонентов безопасности (РКБ) в системе, описываемой на рассматриваемом этапе линейной структурой.

Будем полагать, что РКБ внедрен в систему как объект o_0.

Утверждение 7 (*о размещении РКБ в линейной системе*). Компоненты безопасности (РКБ) могут быть размещены в системе линейной структуры произвольным образом при условии, что в системе присутствует объект o_0.

Доказательство. Рассмотрим вопрос об установлении целостности объекта системы o_k, $k \le N$.

1. Пусть $k = 1$. В этом случае установление целостности объекта o_1 осуществляется на основании априорно определенной целостности объекта o_0. Для этого с помощью вычислимой функции f_0 определяется связь, устанавливающая целостность объекта o_1: $f(o_0) = o_1$.

2. Пусть $2 \le k \le N$. Тогда, имея в системе объект o_0, можно установить целостность интересующего объекта o_k с помощью связей $f_i(o_i) = o_{i+1}$, $i = \overline{1, k-1}$ и рекурсивно определенной функции

$$\begin{cases} y(0) = f_0(o_0) = o_1 \\ y(i) = S^{n_i+1}_{n_{i+1}+1}(f_{i+1}, f_i) = o_{i+1}, \quad i = \overline{1, k-1} \end{cases} \qquad (4.5.5)$$

где $S^{n_i+1}_{n_{i+1}+1}(f_{i+1}, f_i) = f_{i+1}(o_i, f_i(o_i))$ — оператор суперпозиции.

Выберем произвольным образом объект системы o_i, $1 < i < k$. Выделим из множества объектов системы $O = \{o_i\}_{i=1}^{N}$ два подмножества: $O' = \{o_1, \mathbf{K}, o_i\}$ и $O'' = \{o_{i+1}, \mathbf{K}, o_k\}$.

На множестве O' рассмотрим задачу установления целостности объекта o_i.

Аналогично задаче для множества объектов системы $O=\{o_i\}_{i=1}^{N}$ на множестве O' можно определить связи $f'_j(o_j)=o_{j+1},\ j=\overline{1,i-1}$ и функцию

$$\begin{cases} y'(0)=f'_0(o_0)=o_1 \\ y'(i)=S^{n_i+1}_{n_{i+1}+1}\left(f'_{i+1},f'_i\right)=o_{i+1}, \quad i=\overline{1,k-1}, \end{cases}$$

устанавливающую целостность объекта o_i.

Это возможно, если определена связь f_0, т.е. когда в системе присутствует объект o_0 с достоверно установленной целостностью.

Будем считать, что целостность объекта o_i установлена.

На множестве O'' рассмотрим задачу об установлении целостности объекта o_k. В данном случае определения связей $f''_j(o_j)=o_{j+1},\ j=\overline{i+1,k}$ и функции $\Psi''(j),\ j=\overline{i+1,k-1}$ недостаточно для установления целостности объекта o_k. Необходимо присутствие элемента, целостность которого установлена достоверно. В качестве такого элемента может быть выбран объект системы o_i, в силу того, что его целостность является результатом решения задачи для множества O'.

Итак, у нас имеется возможность вычислить функции Y' и Y'', т. е. можно построить машины Тьюринга T' и T'' с соответствующими функциональными возможностями. Из [13] известна

теорема (*о программировании последовательной композиции*): каковы бы ни были тьюринговы программы *A* и *B*, может быть эффективно построена тьюрингова программа *C* такая, что для всех рассматриваемых слов *P*: *C(P)=B(A(P))*.

В соответствии с теоремой всегда может быть построена последовательная композиция машин T' и T'', а именно, машина T, такая, что $T(o_0)=T''(T'(o_0))=o_k$.

Таким образом, можно установить целостность элемента o_k, опираясь при этом на гарантированную целостность объекта o_i, если только возможно установить целостность отрезка $[o_1, o_i]$, или, что то же самое, опираясь на КБ, помещенный в точке i, возможно установить целостность объектов $\{o_i\}_{i=1}^{i}$.

В силу произвольности выбора объекта o_i, можно утверждать, что полученный результат справедлив для любого i, $1 < i < k$.

4.5.3. Размещение резидентного компонента безопасности при обеспечении целостности технологий с древовидной (иерархической) архитектурой

Для процесса активизации вычислительной системы характерна архитектура, которая может быть представлена в виде упорядоченного корневого дерева как на рис. 4.1, где D_i, $i=\overline{1,m}$ — упорядоченные корневые деревья. Компонентам системы соответствуют вершины дерева D. Возможным связям между компонентами системы соответствуют ребра дерева. Компонент системы считается активизированным, если существует ребро, исходящее из соответствующей этому компоненту вершины дерева.

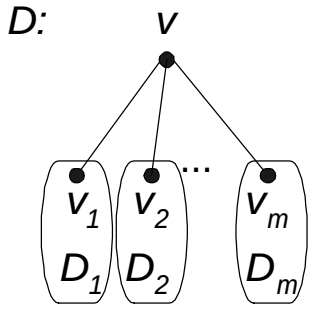
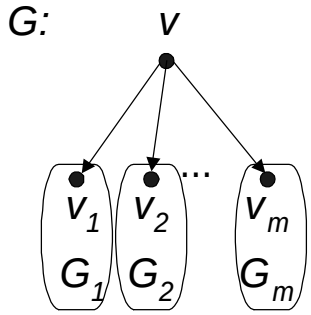


Рис. 4.1

Задача установления целостности рассматриваемой системы эквивалентна задаче установления целостности всех висячих (концевых) вершин дерева *D*.

1. Процесс последовательной по уровням иерархии инициализации системы описывается ориентированным графом *G*, который построен из дерева *D* путем приписывания всем дугам направления от нижестоящей вершины к вышестоящей.



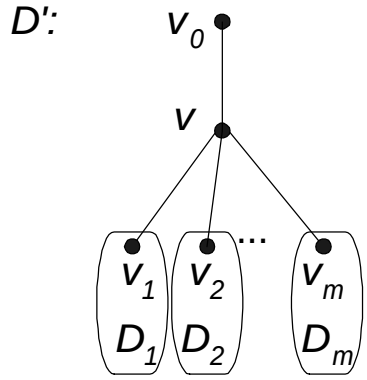
Сначала активизируется компонент системы, соответствующий корневой вершине *v* графа *G*, затем компоненты, принадлежащие второму уровню иерархии, и т. д. При этом инициализация каждой ветви системы, соответствующей одному из подграфов G_i, $i = \overline{1,m}$, осуществляется независимо от всех остальных ветвей системы, которым соответствуют подграфы G_j, $j = \overline{1,m}$, $j \neq i$.

Выберем произвольным образом подграф G_i. Выберем любую концевую вершину из подграфа G_i. Обозначим ее ν_k. Рассмотрим маршрут, а именно простую цепь от корневой вершины ν_i подграфа G_i к выбранной концевой вершине. Очевидно, что простая цепь является единственной. Любой другой маршрут от ν_i к ν_k будет содержать хотя бы одну из вершин и хотя бы одно из ребер не менее 2 раз, т. е. такой маршрут не будет являться простой цепью.

Тогда рассматриваемая задача установления целостности элемента, соответствующего концевой вершине $\nu_k \in G_i$, эквивалентна задаче

установления целостности системы линейной структуры. Эта задача была рассмотрена выше.

Таким образом, для установления целостности элемента $\nu_k \in G_i$ необходимо внедрение в систему специализированного компонента безопасности (РКБ). Причем для рассматриваемой системы РКБ будет определен как вершина ν_0, и тогда система со всеми возможными связями может быть представлена в виде упорядоченного корневого дерева D`.



При этом после последовательной по уровням иерархии инициализации целостность системы будет проконтролирована.

2. Рассмотрим теперь случай, когда инициализация системы выполняется в произвольном порядке. Процесс такой инициализации представляется графом G, который содержит все вершины, присутствующие в дереве D. При этом в силу произвольного порядка инициализации системы говорить о наличии связей между всеми компонентами системы невозможно. Следовательно, в общем случае утверждение относительно наличия или отсутствия любого из ребер графа G невозможно, т. е. граф G будем считать несвязным.

Не ограничивая общности, предположим, что в системе активизированы несколько (n) подветвей. В графе G им соответствуют компоненты связности, т. е. не соединенные друг с другом части. Обозначим их $g_i, i=\overline{1,n}$. Эти компоненты являются связными графами, а именно имеют

структуру упорядоченного корневого дерева. Инициализация ветвей системы, соответствующих компонентам связности $g_i, i=\overline{1,n}$, осуществляется последовательно по уровням иерархии.

В таком случае задача контроля целостности всей системы будет эквивалентна задаче контроля целостности всех активизированных компонентов системы, соответствующих концевым вершинам графа *G*, т. е. концевым вершинам компонентов связности $g_i \in G,\ i=\overline{1,n}$

Выберем произвольным образом один из компонентов связности g_i. Пусть v_0^i — корневая вершина для графа g_i. Тогда согласно случаю, рассмотренному в п. 1., для контроля целостности подветви системы, соответствующей рассматриваемому графу g_i, необходимо разместить специализированный РКБ в вершине v_0^i. Обозначим его КБ$_i$. Аналогично, для контроля целостности всех остальных компонентов связности $g_i \in G,\ i=\overline{1,n}$ необходимо размещение специализированных РКБ в их корневых вершинах $v_0^i,\ i=\overline{1,n}$.

В силу произвольного выбора компонентов связности графа *G* справедливо следующее —

утверждение 8 (*о размещении РКБ в системе произвольной структуры*). Для контроля целостности всей системы в целом необходимо размещение РКБ во всех вершинах графа, кратность которых больше 2, т. е. имеющих по крайней мере 2 ребра, связывающие их с вершинами следующего уровня иерархии.

4.6. Выводы

Концептуальная модель аппаратной защиты технологии электронного взаимодействия базируется на следующих положениях.

1. Для сообщения (документа) выделяются два класса правил — семантические и технологические. Семантические правила определяют требования, гарантирующие, в рамках *социальной среды*, однозначность интерпретации *информации* документа как сведения, смысла, знания. Технологические правила определяют требования к отображению документа в виде объекта или в виде процесса, гарантирующие наличие формальных предпосылок для признания в рамках сектора действенности документа (юридическим) фактом. Только когда технологические требования выполняются, возникают достаточные основания для признания сектором информации *документированной*, а сообщения — документом.
2. Информационная безопасность имеет две составляющих: защиту собственно ЭлД как физического объекта; защиту процессов, реализующих активизированную форму существования ЭлД. Совокупность последних понимается как электронная информационная технология, выбор которой определяется возможностью выполнения эталонных требований, предъявляемых сектором действенности. Назначение защиты процессов обработки информации — гарантировать, что фактически использованная технология соответствует эталонным требованиям, заданным сектором действенности документа.
3. В электронной среде информация определяется как множество (элементов, сигналов) с заданным на нем отношением порядка. Электронная технология также есть строго упорядоченное множество (операций, процессов, процедур) и потому может интерпретироваться как *информация-технология* (в отличие от информации-процесса). В таком случае защита электронной технологии есть защита информации, что объясняет неразрывную связь ее с защитой информации-документа в общем круге проблем обеспечения информационной безопасности. Обеспечивается единая платформа решения проблемы защиты

электронного взаимодействия: *для защиты информации-процесса достаточно защитить информацию-технологию*.

4. Сущность защиты электронной информации, будь то документ или технология, заключается в сохранении изоморфизма между множествами, наблюдаемыми в двух разных точках «пространство-время»: обеспечении и контроле эквивалентности объекта-эталона «на входе» и объекта-результата «на выходе». При защите информации-документа достоверно известен результат — наблюдаемый документ, но имеются крайне ограниченные сведения об исходном ЭлД — объекте-эталоне. В случае защиты информации-технологии, наоборот, достоверно известны характеристики требуемой технологии — эталона, но имеются ограниченные сведения о выполнении этих требований фактически использованной технологией — о результате. Тем самым теоретически обосновывается возможность аппаратной защиты электронной технологии — так как эталон задан и постоянен, то всегда существует принципиальная возможность его реализации в виде предмета — устройства с заданными, фиксированными характеристиками.
5. Аппаратная реализация процесса есть *аналоговый* объект (устройство), физические характеристики которого (множество пар «сигнал на входе — сигнал на выходе») отображают информацию о реализуемом устройством преобразовании. Так как аналоговая форма представления информации имеет несопоставимо более высокую избыточность, нежели цифровая (электронная), то потенциально аппаратные методы и механизмы защиты технологии намного эффективнее программных. В пользу ***hard*** решается один из «основных» вопросов информационной безопасности: «что первично — ***hard*** или ***soft***?» Действительно, ***hard*** есть аналоговая форма процесса, тогда как ***soft*** — электронная (цифровая).
6. Предложена мультипликативная модель информационной безопасности, конкретизирующая ее детерминированные и вероятностные контексты в части угроз и атак. Угроза безопасности ВС есть потенциальная и

постоянно существующая опасность — детерминированное событие, атака как реализация угрозы есть случайное событие. Цель защиты — *отражение атак*, но не противодействие угрозам (как часто считается). Различаются: *защищенность* технологии от угроз как *условная вероятность* отражения атак при нападении; *безопасность* технологии как *безусловная* вероятность технологии сохранять свои номинальные параметры в заданных условиях окружающей среды. Индекс защищенности от множества угроз есть произведение (мультипликация) индексов от каждой угрозы. Безопасность технологии близка к защищенности, если почти наверное угроза в период функционирования ВС реализуется в виде атаки.

7. Исходя из модели изолированной программной среды (ИПС) предложена усовершенствованная субъектно-объектная модель защиты технологии электронного обмена информацией: модель *доверенной вычислительной среды* (ДВС). В отличие от модели ИПС требование неизменности, статичности среды ослабляется до ограничения *целостности*, допускается изменение, динамичность среды в процессе работы. *Под целостностью вычислительной среды понимается стабильность в течение рассматриваемого периода в требуемом диапазоне состава объектов и процессов, их взаимосвязей и параметров функционирования.*
8. Переход от статики в модели ИПС к динамике в модели ДВС концептуально сказывается на вытекающих отсюда методах и механизмах защиты. В принципе изолированность может (а скорее всего — и должна) обеспечиваться без вмешательства в среду, извне. В то же время, любое изменение среды в модели ДВС необходимо должно измеряться для подтверждения того, что оно не вышло за рамки «… требуемого диапазона». В модели ДВС необходимо должен присутствовать компонент безопасности, индицирующий изменения. Поскольку компонент тесно взаимодействует со средой, то целесообразно включить его в состав среды — *резидентный компонент безопасности* (РКБ).

9. Разработана модель размещения РКБ при защите технологий с линейной (последовательной) и иерархической (древовидной) архитектурой. Показано, что РКБ могут быть размещены в системе линейной структуры произвольным образом при условии, что в системе присутствует исходный гарантированно защищенный объект o_0. Если объект o_0 отсутствует, то РКБ должен быть на его месте и выполнять функции исходной «точки опоры». Для контроля целостности технологии с иерархической (древовидной) архитектурой необходимо размещение РКБ во всех вершинах графа, кратность которых больше 2, т. е. имеющих по крайней мере 2 ребра, связывающие их с вершинами следующего уровня иерархии.
10. Задачи безопасности электронного обмена данными, в решении которых должен участвовать РКБ, можно разделить на две группы, соответствующие двум основным этапам работы вычислительной системы:

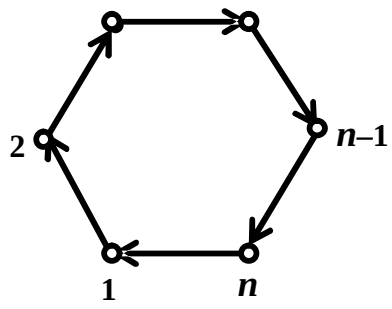
- этап формирования политики безопасности — *режим управления*;
- этап электронного обмена информацией — *пользовательский режим*.

Предметной областью задач первой группы является среда существования документа, целостность и санкционированный доступ к которой должен обеспечиваться средствами защиты — *задачи целостности среды*. Задачи второй группы характерны для *пользовательского режима* работы ВС — *задачи аутентификации объектов и субъектов*. Специфика групп обусловлена *качественно разными* объектами защиты — среда и документ, и, соответственно, должна отражаться в требованиях к РКБ, участвующих в их решении.

11. Установлены принципы реализации РКБ в виде физического устройства:

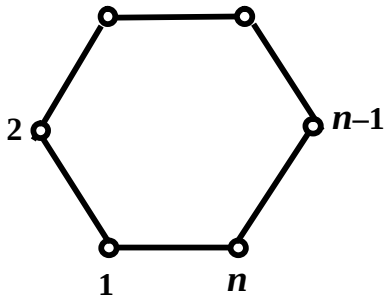
- Реализуя функции эталона, РКБ по сути своей должен представлять собой устройство памяти с очень высоким уровнем защищенности.

- Находясь в рамках электронной среды и взаимодействуя с ее компонентами, РКБ необходимо должен быть вычислительной машиной Тьюринга.
- Для полноценного контроля и защиты вычислительной среды РКБ должен быть максимально независим (автономен) от состояния защищаемой ВС.
- Для достижения высокого уровня защищенности РКБ должен иметь много меньше уязвимостей по сравнению со средой. РКБ необходимо должен быть *узко специализированным*, *примитивным* компьютером.
- РКБ в различные непересекающиеся периоды функционирования ВС должен обеспечивать различные наборы вычислительных операций: в режиме управления W — запись, адрес; в пользовательском режиме R — чтение, адрес.
- В таком случае РКБ может не быть машиной Тьюринга в *краткосрочном* периоде, но должен являться таковой в *долгосрочном*. РКБ может иметь перестраиваемую в зависимости от режима ВС архитектуру.
- Сигнал перестройки не должен выдаваться защищаемой ВС. Перестройка архитектуры РКБ должна осуществляться извне — защищенным воздействием уполномоченного лица.



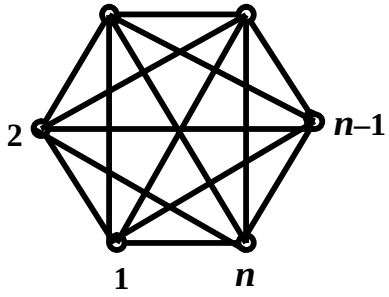
A. — Ориентированное кольцо

$\alpha = 2, \quad b \cong n/2$



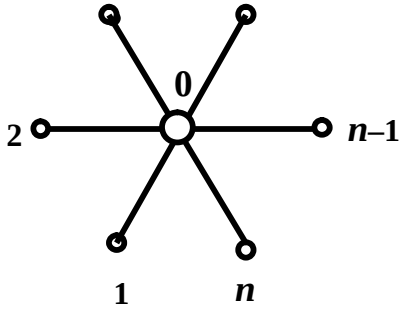
B. — Неориентированное кольцо

$\alpha = 3, \quad b \cong n/4$



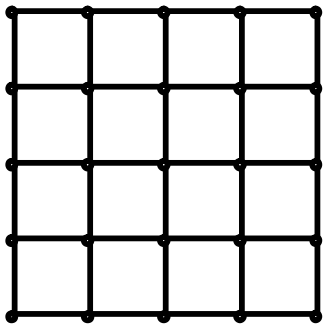
C. — «Каждый с каждым»

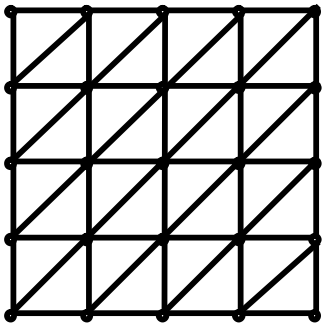
$\alpha = n, \quad b = 0$



D. — Радиальная, «звезда»

$\alpha = 3 + 1/n, \quad b = 1$

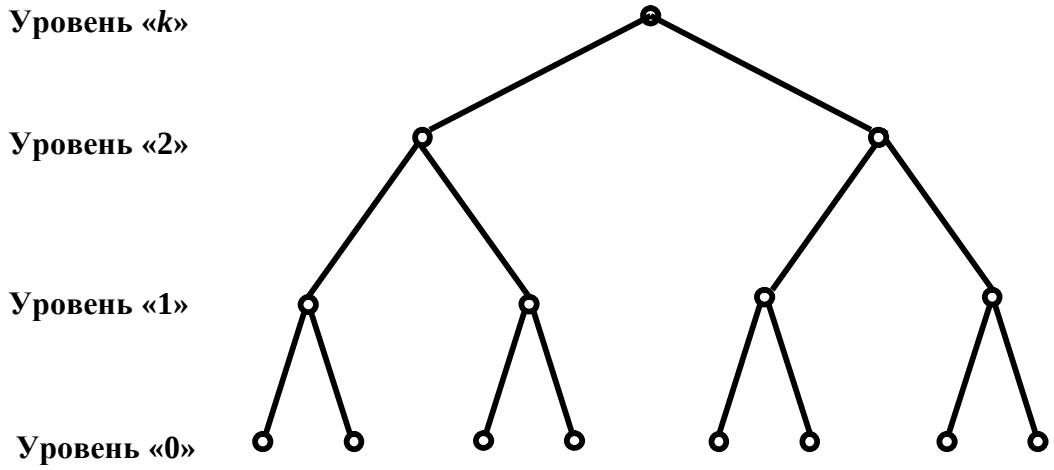




E. — Планарная (с квадратными, треугольными ячейками)

(a — средняя степень вершин в графе сети, n — число объектов сети)

$\alpha = a + 1, \; b \cong 0,667\sqrt{n}$ $\qquad\qquad$ $\alpha = a + 1$



F. — Иерархическая (древовидная)

(a — среднее значение коэффициента разветвления, k — число уровней, n — число объектов системы, $n = a^k$)

$$a = \frac{1}{a^k}\left[\frac{(a+2)(a^k-1)}{(a-1)}-1\right]+2\square 3+O(\frac{1}{n})$$

$$b = k+\frac{k}{a^k-1}-\frac{1}{a-1}\square k-\frac{1}{a-1}+O\left(\frac{1}{n}\right)$$

Рис. 5.1. Наиболее распространенные топологии структур электронного взаимодействия

(a — избыточность механизма аутентификации;
b — среднее число промежуточных ретрансляций).

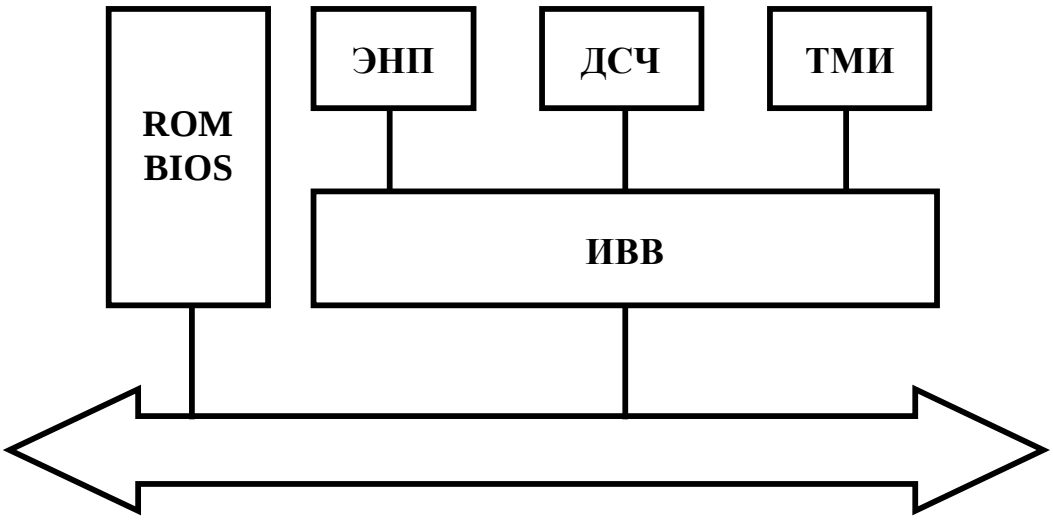


Рис. 5.2. Примерная структура контроллера при аппаратной реализации функции аутентификации в электронной среде
(ЭНП — энерго–независимая память; ДСЧ — датчик случайных чисел; ТМИ — touch–memory интерфейс; ИВВ — интерфейс связи с ЭВМ)

Глава 5. **ПРИНЦИПЫ АППАРАТНОЙ РЕАЛИЗАЦИИ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ В ЭЛЕКТРОННОЙ СРЕДЕ**

Задача аутентификации анализируется в предпосылке электронного обмена информацией, так что далее, если это специально не оговаривается, говорится только об электронной (цифровой) форме ЭлД.

5.1. Понятия идентификации и аутентификации

Понятия «идентификация» (identification — отождествление) и «аутентификация» (authentification — подлинность) близки. В аналоговой среде, обычно используется первое. «Подлинность» может трактоваться очень широко: вряд ли можно считать подлинным документ Президента, доставленный обычным прохожим, а не спецкурьером. В электронной среде, требующей однозначности, такое совмещение смыслов может приводить к абсурдным результатам. Не случайно, что термин «аутентификация» стал широко использоваться именно в сфере электронного взаимодействия. Необходима конкретизация терминов.

Идентификация объекта есть установление (отношения) эквивалентности между объектом и его априорным обозначением (определением, представлением, образом, комплексом характеристик). Иными словами, идентификация есть *опознание*, выделение объекта, приписывание ему априорно известного комплекса характеристик. Можно идентифицировать знакомого из группы стоящих людей, искомый документ из подшивки. Идентификация документа есть установление факта наличия в нем блока *идентифицирующей* информации, выделяющей данный документ среди остальных: наименование отправителя, получателя, тематика, время регистрации и т. п.

Современные ЭВМ являются машинами тьюрингового типа, операция замены символа в подобных машинах — базовая. Следовательно, возможность модификации ЭлД есть принципиальное, *неотъемлемое*

свойство электронного взаимодействия. Соответственно необходимо возникает задача подтверждения идентифицирующей информации, приведенной в документе. Например, что именно указанный в ЭлД субъект действительно является автором или отправителем данного документа, что время регистрации соответствует фактическому и др. Надо «*привязать*» документ как предмет или процесс к субъектам, объектам и процессам, существующим независимо и вне документа, *аутентифицировать* документ.

Когда говорят, что требуется идентифицировать автора, то обычно подразумевают аутентификацию документа. Автор — это не документ, это совершенно другой объект, человек.

В общем случае существенно не только, кто документ сформировал, но и кто документ отправил. Поэтому, оформление документа должно предусматривать, в соответствии с требованиями сектора его действенности, и возможность аутентификации законченных технологических операций формирования, обработки и передачи документа в цикле информационного обмена. При электронном взаимодействии может потребоваться не только аутентификация субъекта аналоговой среды, но и объекта электронной среды, промежуточного процесса обработки ЭлД, программно-технического устройства, на котором был сформирован ЭлД, и т. д.

Аутентификация причастного к документу объекта или процесса (автор, отправитель, получатель, оператор, процесс, технология и пр.) — объективное подтверждение содержащейся в документе идентифицирующей информации об этом объекте или процессе.

Аутентификация *в электронной среде* подразумевает, что все «действующие лица», объекты и процессы, необходимо являются ее элементами. Но это лишь часть *среды аутентификации документа*, включающей еще и аналоговую среду. Например, пусть ЭлД есть запрос на

доступ в некий закрытый фрагмент электронной среды — пароль пользователя. Запрос формируется интерфейсной частью электронной среды — согласно нажатию клавиш пользователем в аналоговой среде происходит создание ЭлД в среде электронной. Какие клавиши нажимать и в какой последовательности, определяет не электронная среда, а *пользователь*. В *аналоговой* среде решается задача выбора пароля — присвоение данному пользователю *y* идентификатора (пароля!) — числа *i*.

А вот предоставлять доступ или нет, решается в рамках собственно электронной среды, на основе анализа поступившего из интерфейсного фрагмента среды *электронного* документа, представляющего собой некоторое двоичное число *x*. Разумеется, число *x* не совпадает с *i*, так как ЭлД содержит еще и массу служебной и технологической информации. Производя регламентированные преобразования числа *x*, т. е. вычисляя заданную функцию *i*(*x*), ЭВМ находит значение *i* и сравнивает его с хранящимися в памяти. При положительном результате сравнения говорят, что пользователь *y* аутентифицирован. Хотя на самом деле аутентифицирована последовательность нажатия клавиш, а кто именно их нажимал — для электронной среды не имеет значения. В таком случае и число *i* — это идентификатор не конкретного пользователя *y*, но *конкретной реализации* электронного процесса формирования пароля. В обиходе эти понятия часто смешиваются, что может приводить к серьезным ошибкам.

Если *гарантируется*, что доступ к среде могут иметь только два пользователя, то для их идентификации необходимо и достаточно всего один бит информации, 0 или 1. Следует ли отсюда, что достаточен одноразрядный идентификатор — пароль длиной в один двоичный бит? Да, если оба пользователя «честные», каждый пользователь инициирует единственный, присущий ему процесс запроса. Нет, если пользователь «нечестный», тогда он может инициировать любой ЭлД-запрос, но

вероятность ошибочной аутентификации будет недопустимо высокой. Два взаимоисключающих ответа на один вопрос возможны, если вопрос некорректен. Выходит, что *аутентифицируется не пользователь, но запрос*: хотя количество пользователей сохранилось, число возможных запросов от каждого увеличилось.

Очевидно, что если пароль сделать длиной в n бит, то вероятность «угадывания» одним пользователем пароля другого снижается до 2^{-n}, и на «вход» процедуры аутентификации возможно поступление 2^n чисел. Даже из этого простейшего примера становится очевидным, что в электронной среде аутентификация *единичных* объектов или процессов сводится к анализу *множества* различных чисел.

5.2. Аутентификация и классификация как эквивалентные задачи

Практический опыт показывает, что в ряде случаев для решения простой задачи необходимо ее усложнить — рассматривать более общую постановку. Можно вспомнить задачу квадратуры круга, бесплодность решения которой оказалась тривиальным следствием кардинально разной природы иррациональных и трансцендентных чисел. Или многолетние поиски аналитических методов нахождения корней многочленов целой степени — невозможность такого решения для уравнений выше четвертой степени вытекает из теории групп. В математике настолько часто, что это кажется неслучайным, справедливо: «для того чтобы решить задачу необходимо выйти на уровень выше».

Исходя из такой посылки, кажется небесполезным переход от анализа аутентификации *одного* заданного документа к исследованию аутентификации всех документов из заданного *множества* — к *классификации* документов. Отнесение некоего объекта к определенному классу представляет собой (если класс называть — «автор», а объект —

«документ») аутентификацию автора этого документа. Но, в традиционном толковании, задачи классификации и аутентификации определены на *разном* предметном поле: *множество* объектов разбивается на *множество* классов, тогда как при аутентификации *одному* документу ставится в соответствие *единственный* автор.

Конечно, это не императив, можно привести большое число примеров, когда усложнение задачи, переход к более высокому уровню обобщения, не компенсируется общностью методов. Корни уравнения 10-й степени $x^{10} = 1024$ очевидны, +2 и –2 кратностью пять, хотя в общем случае уравнения 10-й степени аналитического решения не имеют. Тем не менее, в свете интерпретации электронной среды как пространства чисел и функций, возможность сведения задачи аутентификации к классификации игнорировать ошибочно.

Отображение множества на множество, согласно предыдущему разделу, есть *функция*, тогда как для пары чисел функциональная зависимость бессмысленна. Возникает дополнительная возможность использования не только свойств чисел, но и функций. Число — это статика, тогда как отображение — динамика. В какой-то мере масштаб расширения возможностей можно сопоставить с введением дифференцирования и интегрирования при описании процессов и явлений. При решении задачи классификации потенциально возможно применение несравнимо более мощных математических методов, чем при решении традиционной задачи аутентификации. Каноническая постановка задачи классификации определяется следующим образом:

Классификация данного множества X есть разбиение его элементов x на взаимно непересекающиеся подмножества (классы) X_y*:*

$$X = \bigcup_{y \in Y} X_y,\ X_y \cap X_z = \varnothing, \quad y, z \in Y.$$

Множество X классифицируемых элементов $x \in X$ и множество классов $y \in Y$ заданы. В соответствии с предыдущим можно полагать, что это числовые множества. На множестве X (для всякого $x \in X$) определяется отображение — признак эквивалентности $i(x)$, значение (наблюдение или измерение) которой для данного x позволяет решить, к какому подмножеству (классу) X_y должно его отнести. Говорят, что на X определено отношение эквивалентности i. Под обозначением «$a \sim b$» понимается, что элементы a и b эквивалентны, принадлежат одному классу. Отношение эквивалентности i нельзя выбрать произвольно, должно обеспечиваться выполнение следующих требований (аксиом) [67]:

- аксиома *рефлексивности* — $a \sim a$ для всякого элемента $a \in X$;
- аксиома *симметричности* — если $a, b \in X$ и $a \sim b$, то $b \sim a$;
- аксиома *транзитивности* — если $a, b, c \in X$ и $a \sim b$, $b \sim c$, то $a \sim c$.

Эти условия необходимы и достаточны для того, чтобы отношение i (признак!) позволяло разбить множество X на классы X_y; $X = \bigcup_{y \in Y} X_y$: $\forall y, z \in Y,\ X_y \cap X_z = \varnothing$.

Для того, чтобы два элемента x_1 и x_2 множества X входили бы в *одно и то же* подмножество X_y, должно быть основание: они необходимо должны иметь *в каком-то смысле* одинаковый признак i, являться, в этом контексте, *эквивалентными*. Это не означает, что обязательно $i(x_1) = i(x_2)$, достаточна принадлежность значений их признаков эквивалентности к заданному подмножеству I_y чисел множества I. Например: $x_1 \sim x_2$, если $i(x_1), i(x_2) < I_y$; легко видеть, что все аксиомы эквивалентности здесь выполняются. Точно также должны быть основания и для отнесения элементов к разным классам. Для этого необходимо, чтобы их признаки эквивалентности i отличались, иначе элементы были бы в одном классе, что противоречит исходной посылке.

Итак, разбиение множества X на классы X_y — классификация X, сводится к:

- заданию на множестве X функции $i(x)$ с областью определения $x \in X$ и областью значений $i \in I$, такой, что $I = \bigcup_{y \in Y} I_y : \ \forall y, z \in Y,\ I_y \cap I_z = \varnothing$;
- вычислению признака $i(x)$ для каждого элемента x — нахождению пары $d = \langle x, i(x) \rangle$;
- нахождению подмножества I_y, такого, что второй элемент пары d, признак $i(x) \in I_y$, и отнесению элемента x к классу X_y.

Рассмотренная задача характеризуется одним признаком эквивалентности $i(x)$, будем называть ее, при необходимости конкретизации, *одномерной классификацией*. Задача очевидным образом обобщается на случай нескольких признаков эквивалентности, и тогда можно говорить о *многомерной* классификации. Формально подобная детализация избыточна и рассматривается здесь только для обоснования в дальнейшем направлений практического решения. Действительно, в случае одномерной классификации пространство X отображается на одномерное пространство (множество классов) Y, точка которого $y \in Y$ есть одно число. Тогда как при m-мерной классификации множество Y есть многомерное пространство, каждая точка которого $y \in Y$ есть совокупность m чисел.

На множестве $x \in X$ задается m функций эквивалентности $i_1(x), i_2(x), \ldots, i_m(x)$, области значений которых есть, соответственно, $I_1, I_2, \ldots, I_m$. Для каждого x вычисляется m-мерный признак эквивалентности $i = |i_1, i_2, \ldots, i_m|$, упорядоченное множество частных признаков. Значение i является основанием для отнесения данного x к одному из классов I — прямого произведения множеств $I = I_1 \times I_2 \times \ldots \times I_m$. Если разрядность любого частного признака эквивалентности ограничена, то совокупность $|i_1, i_2, \ldots, i_m|$ m чисел можно записать как их конкатенацию

в виде одного числа $i = i_1||i_2|| \ldots ||i_m$. Таким образом, многомерная классификация сводится к одномерной.

В зависимости от числа градаций каждого из признаков эквивалентности, их взаимообусловленности, мощности подмножеств, обладающих каждым из признаков, и пр., конкретная реализация многомерной классификации может иметь те или иные преимущества. Однако сущность необходимо одинакова — это каноническая задача разбиения множества на подмножества.

Пусть теперь классифицируется множество D, каждый элемент которого $d \in D$ есть пара чисел $d = \langle x, i(x)\rangle$. Если называть D документом, $x \in X$ — текстом документа d, а признак эквивалентности $i(x)$ — идентификатором автора $y \in Y$ документа d, то классификация D сводится к установлению для каждого «документа» x из X «автора» y из Y. Множества X и Y — это разные множества, а процедура классификации есть процедура, объективная по определению — в силу математических методов решения. Следовательно, определение класса элемента x есть *объективное подтверждение содержащейся в документе* d *информации* $i(x) \in I_y$ *об авторе* y. Решается задача аутентификации «*причастного*» к x согласно признаку эквивалентности $i(x)$ элемента y, лежащего *вне* X. Столь же очевидно и обратное рассуждение, показывающее, что возможность аутентификации любого x позволяет классифицировать множество X.

Так как числа x и $i(x)$ принадлежат разным множествам, то они «отделимы» друг от друга: одно из чисел пары $d = \langle x, i(x)\rangle$ может быть искажено. Физически это означает, что документ $d = \langle x, i(x)\rangle$ заменяется поддельным $\overline{d}$, в котором подделан текст и/или автор: $\overline{d} = \langle \overline{x}, i(x)\rangle$, или $\overline{d} = \langle x, i(\overline{x})\rangle$, или $\overline{d} = \langle \overline{x}, i(\overline{x})\rangle$.

Задачи аутентификации и классификации сводятся к эквивалентным постановкам. Но это означает, что в принципиальных

положениях должны совпадать и методы решения. А поскольку при классификации не обойтись без задания функций (корректнее, отображений) эквивалентности, то и при аутентификации неизбежен выход в пространство функций. И если на практике это не очевидно в явном виде, то *всегда* может быть установлено при более тщательном анализе любой успешной процедуры аутентификации.

5.3. Прикладные особенности аутентификации в агрессивной среде существования электронного документа

Хотя классификация и аутентификация теоретически эквивалентны, с прикладной точки зрения следует отметить ряд особенностей этих процедур. Очевидно различие в размерности: классифицируются *все* элементы множества X, а аутентифицируются *отдельные* элементы $x \in X$. И если мощность множества $|X|$ бесконечна, то его классификация за конечное время на практике невозможна, в то время как аутентификация любого элемента реализуема.

На практике это не существенно: всегда можно ограничить разрядность чисел-документов x, что автоматически означает конечность мощности $|X| = n < \infty$. При любой конечной мощности $|X|$ зависимость между вычислительной сложностью классификации и аутентификации *линейна*. В теории сложности вычислений считается, что если количество операций (длина ленты) на машине Тьюринга для реализации алгоритма решения имеет полиномиальную зависимость, $O(n^k)$, от размерности n задачи, то ответ достижим на практике, если выше, (суб)-экспоненциальную $O(e^n)$ или факториальную $O(n^n)$, то — нет. Следовательно, алгоритмы классификации и аутентификации реализуемы или нет одновременно: решается одна задача — решается и другая.

Более значимым отличием традиционных постановок является то, что при классификации множество элементов X и множество классов Y *задается*, а при аутентификации — *предполагается* по умолчанию, описывается контекстно, неявно: задаются *единственный* элемент $x \in X$ и *единственный* элемент $y \in Y$. В то же время, переход в пространство функций эквивалентности требует *задания* области определения X и области значений Y. Для корректного сведения процедур аутентификации к классификации необходимо доопределить эти множества.

Прежде всего, уточним, о каких множествах идет речь. Любой документ x создается или формируется автором y в одной точке системы координат «пространство-время» — точке формирования, но аутентифицируется в другой — точке аутентификации. Абсолютные значения координат несущественны, важно только различие точек, поэтому можно поставить в соответствие точке формирования любого документа значение «0», а точке аутентификации — значение «1». Таким образом, в точке «0» множество авторов Y *формирует* множество документов X, тогда как в точке «1» *классифицируется* множество X_1 по классам множества Y_1. При этом никаких ограничений на совпадение множеств в точках формирования и аутентификации не накладывается, т. е. в общем случае $X \neq X_1$, $Y \neq Y_1$.

Это означает, что каждому документу $d = \langle x, i \rangle$ из множества $X = \{d\}$ в точке «0» соответствует в точке «1» подмножество $d \cup \bar{d}$ множества X_1, где $\{\bar{d}\} = \{\langle \bar{x}, i \rangle, \langle x, \bar{i} \rangle, \langle \bar{x}, \bar{i} \rangle\}$ — множество «поддельных» документов, порожденных данным документом d и отличающихся от него искажением либо текста $\bar{x}$, либо идентификатора $\bar{i}$, либо тем и другим сразу. Возможность подделки обусловлена случайным или злонамеренным воздействием на документ на этапе его жизненного цикла между точками

«0» и «1». Таким образом, множество X_1 есть объединение $X_1 = X \cup \bar{X}$, где $\bar{X} = \mathop{\mathbf{U}}_{\langle x,i\rangle}\left\{\left\langle x,\bar{i}\right\rangle,\left\langle \bar{x},i\right\rangle,\left\langle \bar{x},\bar{i}\right\rangle\right\}$ — множество всех поддельных документов.

В зависимости от особенностей множеств документов и авторов в точках формирования и аутентификации различаются три класса среды аутентификации: достоверная, случайная, агрессивная. В *достоверной* среде всегда $X = X_1$, $Y = Y_1$, т. е. возможные искажения текста и идентификатора документа исключены (практически незначимы). В таком случае классификация на основе единственного признака эквивалентности достаточна для аутентификации любого ЭлД, и документ представляется в виде пары $d = \langle x, i\rangle$.

В *случайной* среде аутентификации допускается искажение *не более чем одного* из элементов пары: если в точке формирования «0»имеется документ $d = \langle x, i\rangle$, то в точке аутентификации «1» аутентифицируются порождаемые им документы — множество $d \cup \bar{d}$, где $\{\bar{d}\} = \{\langle \bar{x},i\rangle, \langle x,\bar{i}\rangle\}$. Для аутентификации необходимо классифицировать множество X, поэтому в точке «1» множество X_1 предварительно надо разделить еще на классы X и $\bar{X}$ — двухмерная классификация. Для этого нужен еще один признак эквивалентности h, т. е. необходимо документ, формируемый в точке «0», должен представлять собой трио $d = \langle x, i, h\rangle$, где $h = h(x, i)$, или $h = h_i(x)$, или $h = h_x(i)$. Обычно h есть хэш-код содержания x и идентификатора i, тогда атрибут h достаточен для индикации случайных воздействий на документ, когда *согласованное* искажение *всех* элементов трио $\langle x, i, h\rangle$ практически невозможно.

Однако, в *агрессивной* среде аутентификации злонамеренное воздействие при несанкционированном доступе делает такое возможным, если, например, хэш-функция $h = h(x, i)$ общедоступна и известна злоумышленнику. Тогда множество $\bar{X}$ будет объединением двух

непересекающихся подмножеств $\bar{X} = \bar{X}^{*} \cup \bar{X}^{**}$, где $\bar{X}^{*}$ — подмножество поддельных документов со случайными искажениями, а $\bar{X}^{**}$ — подмножество поддельных документов со злонамеренными искажениями. Возникает еще одно измерение: трехмерная классификация. Рассуждая аналогично, приходим к выводу, что документ должен формироваться уже в виде квартета $d = \langle x, i, h, p \rangle$, где p — индикатор некой защиты, связывающей элементы трио $\langle x, i, h \rangle$.

Возможны различные конструкции функций h, p, приводящие к различным классам механизмов аутентификации — код аутентификации, пароль, ЭЦП.

В зависимости от доступности атрибутов ЭлД и требований к ошибке аутентификации можно, рассуждая по индукции, прийти к необходимости формирования документа с большим числом признаков эквивалентности. Но в любом случае рост их числа в агрессивной среде заканчивается «секретным» признаком — эквивалентом «пароля» автора, ключа шифрования и/или подписи и др.

Полученный результат о необходимости нескольких атрибутов ЭлД для его надежной аутентификации не противоречит установленному ранее положению о сводимости многомерной классификации к одномерной: несколько чисел-признаков можно представить в виде одного числа, объединив их посредством конкатенации. Всегда можно считать, что документ характеризуется единственным *обобщенным* идентификатором, одна часть которого является общедоступной, а другая — секретной, далее называемой «паролем» пользователя.

Итак, в агрессивной среде аутентификации электронного документа идентификатор документа необходимо должен содержать, в явной или неявной форме, защитный (возможно, криптографический) атрибут, известный получателю документа. Очевидно, что пароль должен быть известен *минимальному* количеству «посторонних» — *принцип*

минимизации избыточности секретной информации. Применение принципа позволяет сравнить различные топологии аутентификации и сформировать требования к предпочтительной архитектуре механизмов аутентификации ЭлД в агрессивной среде.

Пусть электронный обмен организуется в системе, включающей n объектов (пользователей), и необходимо обеспечить взаимодействие каждого с остальными. Несекретная часть идентификатора в соответствии с определением аутентификации понимается как «идентифицирующая информация» об авторе документа — аутентифицируемом причастном к документу объекте или процессе. Секретная часть идентификатора есть ресурс для «объективного подтверждения» этой информации.

Сравним наиболее распространенные схемы организации аутентификации в таких системах: полносвязная (каждый с каждым), ориентированная и неориентированная кольцевая, радиальная (звезда), планарная сеть, древовидная (иерархическая). Оценим минимально необходимый суммарный объем секретной информации, который должен быть известен для обеспечения аутентификации документов объектами системы при взаимодействии друг с другом.

В первом приближении это можно оценить суммарным количеством паролей (с учетом повторений), которые должны быть известны участникам: если один и тот же пароль известен двум участникам, то его надо учитывать дважды. «Каждый может проболтаться», следовательно, и несанкционированный доступ к паролю становится «вдвое проще». Обозначим удельный объем закрытой информации в расчете на один объект через α и будем называть эту величину α *избыточностью* механизма аутентификации, в том смысле, что в достоверной среде аутентификации избыточность $\alpha = 0$, так как необходимость в *дополнительной* информации, подтверждающей открытый идентификатор, здесь отсутствует.

Минимальное значение избыточности очевидно, хоть какой-то секрет у каждого из взаимодействующих объектов должен существовать, следовательно, $\alpha_{min} = 1$. На практике такой минимум достигается асимметричными методами криптографии, применение которых обычно подразумеваемых по умолчанию, когда говорят о механизмах электронной цифровой подписи — ЭЦП. При этом возможно непосредственное взаимодействие объектов, так что среднее число промежуточных ретрансляций $\beta = \beta_{min} = 0$.

Для симметричных методов минимальное значение избыточности определим на основе следующих рассуждений: для того чтобы в замкнутой группе из n людей «выйти на нужного человека», каждому необходимо знать, как минимум, еще одного постороннего человека. Это означает, что любой из n объектов системы должен «знать», как минимум, два идентификатора–пароля: свой собственный и один посторонний. Таким образом, суммарный объем секретной информации (количество паролей), которая известна объектам системы, не может быть ниже $2n$, соответственно $\alpha_{min} = 2$. Не имеет значения, каким образом организуется взаимодействие в такой системе, несомненна только ретрансляция документа: адресат известен из открытой части идентификатора, но кто-то должен поручиться за «объективность информации, идентифицирующей автора ЭлД», и это поручительство выражается в подтверждении такой информации собственным идентификатором ретранслятора.

Теперь перейдем к анализу наиболее распространенных структур взаимодействия. Если взаимодействие осуществляется в архитектуре «*ориентированное кольцо*» (Рис. 5.1А), то каждый объект должен хранить в тайне собственный пароль (защитный код аутентификации — ЗКА), чтобы им не воспользовались посторонние, и знать ЗКА соседа, чтобы объективно установить отправителя документа. Для системы «ориентированное кольцо» $\alpha = 2$. Поскольку при каждой ретрансляции

осуществляется доступ к ЭлД, пусть и санкционированный, то число ретрансляций также влияет на выбор схемы аутентификации: при равновероятном трафике между объектами среднее число ретрансляций $\beta \cong (n-1)/2$. С увеличением числа объектов системы число ретрансляций возрастает, что упрощает несанкционированный «съем» информации и, соответственно, негативно сказывается на аутентификации. Избыточность возможных путей взаимодействия ухудшает достоверность аутентификации, но улучшает другие параметры — сокращается среднее число промежуточных ретрансляций документа. При схеме «*неориентированное кольцо*» (Рис. 5.1B), избыточность $\alpha = 3n / n = 3$, но число ретрансляций сокращается вдвое, $\beta \cong (n-1)/4$.

При схеме взаимодействия «*каждый с каждым*» (Рис. 5.1C) ЭлД не нуждается в ретрансляции, $\beta = 0$, однако каждый объект должен «знать» как свой пароль-идентификатор, так и пароли каждого из остальных $n-1$ объектов системы. Избыточность $\alpha = n^2 / n = n$. Возможности несанкционированного доступа линейно увеличиваются с ростом числа объектов системы, что делает такой механизм приемлемым только для малых систем.

При *радиальной* топологии системы, типа «*звезда*» (Рис. 5.1D), каждый из объектов должен «знать» два пароля — собственный и центра, а центру кроме своего пароля должны быть известны пароли–идентификаторы всех n объектов системы. Избыточность механизма «звезда» равна $\alpha = (2n + n + 1) / n = 3 + 1 / n$, почти такая же, как при кольцевой топологии, но при связи любых объектов отсутствует ретрансляция, $\beta = 0$. Как избыточность α, так и среднее число ретрансляций β при информационном обмене невелики и практически не зависят от размера системы, что делает механизмы аутентификации такого

типа весьма перспективными для небольших и средних систем электронного взаимодействия.

Однако в больших системах подобный механизм резко увеличивает вероятность «катастроф», так как в центре скапливается слишком много секретной информации о паролях *всех* объектов системы. Утечка информации из центра может привести к параличу всей системы, не говоря уже о сложности технологических и технических проблем практической реализации подобной схемы при большой пространственной разнесенности объектов системы.

Таких недостатков лишены механизмы аутентификации с *древовидной* (*иерархической*) структурой. Для простоты рассмотрим структуру с k уровнями иерархии и постоянным коэффициентом a разветвления на любом уровне иерархии (Рис. 5.1E, $k = 4$, $a = 2$). Общее число объектов системы $n = a^k$. Можно показать, что в таких иерархических механизмах аутентификации при больших $n = a^k$ избыточность α будет примерно такой же, как при кольцевой топологии:

$$\alpha = \frac{1}{a^k}\left[\frac{(a+2)(a^k-1)}{(a-1)} - 1\right] + 2 \approx 3 + O\left(\frac{1}{a^k}\right) \approx 3 + O\left(\frac{1}{n}\right).$$

Среднее число ретрансляций β при равновероятном трафике между объектами системы растет как логарифм числа объектов. В рассматриваемом случае

$$\beta = k + \frac{k}{a^k - 1} - \frac{1}{a-1} \approx k - \frac{1}{a-1} + O\left(\frac{1}{n}\right).$$

При *планарной* топологии система отображается в виде сети, например, решетка с треугольными или квадратными ячейками (Рис. 5.1E).

Обозначим через a среднюю степень вершин графа сети, т. е. среднее число объектов, с которым непосредственно соединяется данный объект. Тогда любой объект, кроме собственного, должен «знать» пароли-идентификаторы всех смежных объектов. Избыточность для подобной схемы аутентификации находится очевидным образом, $\alpha = [n(a + 1)] / n = a + 1$. Сложнее задача оценки среднего числа β ретрансляций в такой системе. При равновероятном трафике между объектами величина β зависит от конкретного вида ячеек сети. При квадратных ячейках и большом числе объектов можно показать, что значение β растет как квадратный корень из общего числа n объектов сети: $\beta \cong 0,667\sqrt{n}$.

Представленный анализ показывает, что с позиций аутентификации целесообразна организация документооборота по радиальной (при умеренном количестве взаимодействующих объектов) или иерархической схеме (при большом числе объектов, сгруппированных в различных точках пространства). Только тогда избыточность и количество ретрансляций принимают умеренные значения, причем не зависящие или почти независящие от числа объектов. При такой архитектуре информация, как-то эквивалентная паролю аутентифицируемого пользователя, объекта или процесса электронной среды, может храниться концентрировано. Например, в виде таблиц (достоверности) в защищенной энергонезависимой памяти сервера безопасности.

Ранее было установлено, что только при условии неизменности защищаемого объекта, при выполнении им функции эталона, аппаратная реализация технологии в силу постоянства, присущего материальным объектам, имеет преимущества по сравнению с программными механизмами. В таком случае вопрос о применимости аппаратных механизмов для аутентификации ЭлД нетривиален. Если исходить из

традиционной трактовки, рассматривать аутентификацию *одиночного* конкретного ЭлД, то ответ отрицательный: все документы различны, и ни о каком постоянстве речи быть не может. Но, как показано, аутентификация эквивалентна классификации, а предметная область классификации есть *множество* документов, поэтому необходимо должно существовать нечто общее, постоянное, в процессе классификации, соответственно — и аутентификации. Именно это «общее» и может являться предметной областью аппаратной реализации элементов технологии аутентификации.

Отображение любого ЭлД как пары $d = \langle x, i \rangle$ (x — текст, $i = i(x)$ — идентификатор) всегда возможно в силу сводимости многомерной классификации к одномерной. В этой паре текст x меняется от документа к документу, тогда как идентификатор i, хотя и связан с переменным x, но характеризует *один и тот же* аутентифицируемый объект или процесс, и потому должен быть *в каком-то смысле* постоянен в пространстве и времени, например, пароль, ключ. Таким образом, одним компонентом предметной области защиты аутентификации могут являться секретные данные (числа) идентификатора аутентифицируемого объекта: ключи, пароли. Другой потенциальный компонент определяется второй составляющей электронной среды — алгоритмами, по определению инвариантными к преобразуемой информации. Так как *вычисление* идентификатора i должно быть одним и тем же при различных x, собственно преобразование $i(x)$ должно быть константным. А это означает, что аппаратная защита неизменности $i(x)$ как *отображения* x также целесообразна и перспективна.

В достоверной среде защита аутентификации не нужна — нет атак. Остается рассмотреть агрессивную среду, в которой, как установлено, документ d должен формироваться, как минимум, в виде четырех чисел $d = \langle x, i, h, p \rangle$, где x — собственно документ (текст), i, h, p — атрибуты,

признаки эквивалентности. Функционально *i* и *p* равнозначны; если *i* — имя автора, то *p* в каком-то смысле — его секретный псевдоним. Таким образом, в качестве объектов аппаратной защиты аутентификации можно выделить два условно постоянных параметра: функциональный аналог пароля «автора» *p* и реализацию преобразования *h*, связывающего *x*, *i*.

Аппаратные методы защиты процедур аутентификации ЭлД могут быть эффективны только в части формирования, обеспечения целостности (хранения) и конфиденциальности (как исключения НСД) криптографических ключей (и/или паролей) авторов и целостности (криптографических) преобразований.

Целесообразно оценить границы предпочтительности двух различных классов методов, применяемых при аутентификации документа: симметричных и асимметричных. Для определенности рассмотрим ЭЦП как реализацию асимметричных методов и защитные коды аутентификации (ЗКА), основанные на применении симметричных методов.

Оба класса методов базируются на секретном ключе шифрования; от того, что ключ именуется различно, «закрытый ключ ЭЦП» или «пароль, защитный код аутентификации — ЗКА», суть дела не меняется. В целом можно считать, что, при отсутствии инсайдерской информации о ключах, криптостойкость методов в первом приближении сопоставима. На первый план выходят прикладные характеристики методов: юридические аспекты ответственности за разглашение ключей, возможность получения инсайдерской информации о ключах при несанкционированном доступе или от источников, допущенных к ключам шифрования, эффективность технической реализации шифрования и дешифрования.

Ключи шифрования и дешифрования могут быть одинаковыми, могут вычисляться один из другого, могут быть и принципиально разными, но их всегда два. С другой стороны, чтобы «скрыть»

информацию от посторонних, достаточен всего один ключ. Теоретически возможно обеспечить конфиденциальность, сохраняя в тайне всего один ключ — точнее, один из ключей криптографического взаимодействия может быть, в принципе, несекретным. Это характерно для асимметричных методов: они базируются на разных ключах, один из которых называется «закрытым» и держится в секрете, другой — «открытым». В зависимости от целей взаимодействия «закрытым» может являться как ключ шифрования — если аутентифицируется отправитель документа, так и дешифрования — если получатель.

При симметричных методах либо оба ключа одинаковы, либо один из них легко определяется на основе второго. Такие методы применяются для аутентификации при использовании защитных кодов аутентификации — ЗКА.

В практических применениях ответ на вопрос о предпочтительности построения прикладных механизмов аутентификации далеко не однозначен, несмотря на очевидное преимущество ЭЦП: известности закрытого ключа *одному и только одному* из взаимодействующих объектов. Отсюда вытекают два главных достоинства применения ЭЦП:

- преимущество однозначности — *юридическая* возможность возложения ответственности за сохранение в тайне закрытого ключа на конкретное физическое лицо;
- преимущество потенциально более высокой защищенности — возможность единственного места хранения закрытого ключа.

Конечно, однозначность всегда желательна, но *не всегда необходима*. В технических системах порой проще заменить неисправный блок, чем искать отказавшую деталь. В учреждении зачастую эффективнее ограничить доступ к информации всей группе сотрудников, чем определить, кто из них персонально виновен в утечке. Даже при единственном месте хранения ключа, соблюдении всех правил и

инструкций, единоличной ответственности неизбежно возникают возможности доступа третьих лиц. В этом случае наказание ответственного не повлияет на наличие канала доступа — увольнять надо не ответственного, а «третье лицо» — тогда утечка прекратится.

Преимущество однозначности играет решающую роль, если ответственность за *применение* закрытого ключа не только можно, но и *необходимо требуется* возложить на *единственное* лицо. Вопреки обычному заблуждению, ответственность должна наступать именно *за применение, а не за хранение ключа в тайне*, это разные виды ответственности. Такое возможно только при информационном взаимодействии в социальной среде, где понятие наказания и санкций имеет смысл. Если ЭлД не выходит за рамки электронной среды, то однозначность ЭЦП оказывается не столь существенным фактором: неодушевленный объект нельзя ни наказать, ни поощрить, здесь нет места социальным законам.

Остается преимущество защищенности, и тут необходим более тщательный анализ. Действительно, закрытый ключ ЭЦП можно хранить «в одном месте», но отсюда не следует, что процедуры формирования ЭЦП могут быть столь же сильно локализованы — это весьма трудоемко при реальной длине ключа. Требуется привлечение значительных программно-технических ресурсов, соответственно «расширяется» сектор электронной среды, в котором выполняются необходимые операции, и резко возрастают возможности НСД.

В то же время при симметричных методах преобразования выполняются несравнимо более простыми методами. В свою очередь, это означает, что такие механизмы могут быть реализованы в виде специализированного модуля, а эффективность аппаратных механизмов защиты, как было установлено, потенциально много выше программных. Таким образом, более высокая защищенность ЭЦП по сравнению с ЗКА

при аутентификации объектов электронной среды далеко не очевидна, и выбор средства аутентификации должен учитывать конкретные условия информационного обмена.

Есть еще один веский аргумент в пользу применения ЗКА в вычислительных системах с последовательной, централизованной или иерархической структурой обмена информацией (Рис. 5.1 A, B, D, F), характерной для корпоративных систем. При n взаимодействующих объектов применение ЗКА по сравнению с ЭЦП требует защиты сопоставимого количества информации об идентификаторах. В подобных системах применение аутентификации *электронных* процессов и объектов на основе ЗКА может оказаться, в конечном итоге, более эффективным, чем ЭЦП. При взаимодействии «каждый с каждым» (Рис. 5.1C) приведенный аргумент не столь очевиден: применение ЭЦП требует защиты от НСД n идентификаторов, применение ЗКА — n^2.

И, наконец, последнее обстоятельство в пользу ЗКА — временные затраты на процедуры аутентификации при использовании симметричных и асимметричных методов криптографии отличаются в сотни (программная реализация асимметричной криптосистемы RSA по сравнению с симметричной DES) и тысячи (аппаратная реализация) раз. Если трафик ЭлД незначителен, что присуще функциональным документам — договора, письма, указания и т. п., это не существенно. Но если ЭлД носят технологический характер — обслуживание финансовых потоков, технологические системы управления и др., то ситуация кардинально меняется.

Необходимо разумное сочетание механизмов аутентификации: ЭЦП — на «внешних» сечениях вычислительной системы; ЗКА — на «внутренних».

5.4. Архитектура механизмов аппаратной аутентификации электронного документа

В зависимости от контекста аутентификация понимается либо как *результат*, либо как *процесс* «…объективного подтверждения содержащейся в документе идентифицирующей информации об аутентифицируемом объекте». Соответственно, требованием к реализации механизмов аутентификации является *обеспечение объективности* подтверждения содержащейся в документе идентифицирующей информации об объекте, что, вообще говоря, может и не зависеть от собственно информации. Например, аутентификация автора рукописного документа на основе почерка инвариантна к содержанию документа.

Часто используемая в локальных сетях (например, ЛВС Novell NetWare) система аутентификации ориентирована на подтверждение подлинности пользователей в момент запроса доступа к ресурсам файлового сервера. В качестве базовой системы принята схема с простым паролем пользователя, в то же время подлинности рабочих станций сети уделяется недостаточное внимание: единственная проверка заключается в сравнении номера сетевой карты рабочей станции, с которой идёт запрос доступа, со списком разрешённых сетевых карт для данного пользователя. Все остальные проверки, осуществляемые при диалоге пользователя и файлового сервера, решают одну задачу — проверку подлинности пользователя.

Однако аутентификация только номера сетевой карты при запросе пользователем доступа к ресурсам файлового сервера не пресекает все возможности несанкционированного доступа. Внеся дополнительную строку в файл настройки сетевого программного обеспечения рабочей станции, пользователь может задать любой номер сетевой карты и получить доступ к ресурсам файлового сервера с любой рабочей станции

ЛВС, причем для сервера данное соединение будет корректным. Для рабочих станций, работающих под управлением каких-либо средств защиты от НСД, неконтролируемое изменение номеров сетевых карт может разрушить любой план защиты. Другим путём несанкционированного доступа к ресурсам файлового сервера является подключение посторонней станции к сети. Например, принцип работы ЛВС EtherNet таков, что злоумышленник может незаметно подключить свою ЭВМ к кабелям ЛВС и работать как легальная станция.

Таким образом, отсутствуют конструктивные преграды для несанкционированного доступа к ресурсам файлового сервера с любой рабочей станции в ЛВС. В локальной сети пользователем является вовсе не оператор, а рабочая станция, точнее — оператор *вместе* со станцией, тогда как существующие подсистемы аутентификации ориентированны на установление подлинности только пользователя-*субъекта*. Критичным с точки зрения НСД является как подмена оператора, так и подмена рабочей станции. Следовательно, необходимо применять механизмы аутентификации, обеспечивающие проверку подлинности файловых серверов и рабочих станций *после* того, как пользователь признан корректным с точки зрения Novell NetWare.

Это взаимодействие всякий раз должно содержать уникальные данные, иначе, прослушав один раз такой диалог, злоумышленник сможет полностью воспроизвести его и, в результате, получить доступ к ресурсам файлового сервера. В каждом сеансе аутентификации необходимо использовать «*новые*» случайные данные, которые должны при этом ещё и обеспечивать проверку подлинности обеих сторон. Решение можно обеспечить применением механизма, основанного на коде аутентификации, функционально эквивалентного электронной цифровой подписи. Однако в этом случае возникает не менее сложная задача хранения секретных ключей станций.

С учётом всего перечисленного необходима дополнительная проверка подлинности рабочих станций в момент запроса доступа к ресурсам файлового сервера. Секретный ключ станции хранится в закодированном виде, причём кодируется он на секретном ключе пользователя, который, в свою очередь, должен храниться вне ЭВМ, например, в Touch Memory пользователя. Тогда, даже в случае полного доступа к рабочей станции, у злоумышленника нет никакой возможности получить доступ к секретному ключу станции. Доступ к секретному ключу файлового сервера также должен быть затруднён для посторонних, ключ в максимальной степени должен быть изолирован от общедоступной вычислительной среды. То же самое требование справедливо и для сеансовых ключей, создаваемых для каждого акта электронного взаимодействия. Поскольку любая криптография всегда базируется на случайности, то применение датчика случайных чисел (ДСЧ) в механизмах аутентификации обязательно.

В свете установленных положений становится очевидным, что для аппаратной аутентификации в электронной среде минимальная конфигурация соответствующего резидентного компонента безопасности (РКБ) должна включать в свой состав следующие функциональные узлы (Рис. 5.2):

- touch-memory интерфейс — ТМИ;
- энергонезависимую память — ЭНП;
- датчик случайных чисел — ДСЧ;
- постоянное запоминающее устройство (ПЗУ) пользовательского расширения BIOS — ROM BIOS;
- интерфейс связи с ЭВМ — ИВВ.

Из ТМИ в контроллер поступает информация о пользователе и (в общем случае) контрольная сумма прикладных задач и данных. В ЭНП хранится (как минимум) эталонная информация для процедур

аутентификации пользователя, ссылки на полномочия пользователя и контрольные суммы для контроля целостности системных областей и системных файлов. Датчик случайных чисел используется как генератор необходимых ключей взаимодействия. ROM BIOS должен содержать фиксированное описание преобразований, обеспечивающих:

- блокировку загрузки ОС с отчуждаемых носителей;
- процедуры идентификации (аутентификации);
- процедуры разбора файловой системы;
- процедуры расчета хэш-функции;
- процедуры работы с энергонезависимой памятью и ДСЧ.

Аппаратная реализация в силу физической изолированности обеспечивает эффективную защиту от НСД наиболее важных процедур и данных, используемых при аутентификации ЭлД. Но, разумеется, не всех — в любом случае взаимодействие с вычислительной средой, окружающей РКБ, необходимо должно существовать. Соответственно, предусматривается интерфейс связи с ЭВМ — ИВВ (интерфейс ввода-вывода).

Наличие рассмотренных ресурсов минимально необходимо для аппаратной аутентификации. Реально может потребоваться включение дополнительных возможностей, обеспечивающих потребительские удобства применения РКБ для аутентификации ЭлД.

5.5. Программно-техническая реализация аппаратных средств защиты информации

Выбор системы защиты информации от несанкционированного доступа должен основываться на анализе требований, предъявляемых как к составу функциональных параметров, так и к параметрам производства и

сопровождения изделий, а также к эксплуатационным характеристикам. СЗИ должна отвечать следующим требованиям.

1. В предыдущем разделе были сформулированы основные требования к функциональности и составу аппаратных средств защиты информации (СЗИ) (Рис. 5.1). Это позволяет определить перечень узлов, которые должны быть реализованы в контроллере СЗИ, взаимосвязи межу ними и сформулировать требования к их реализации.

2. Функциональные возможности СЗИ должны обеспечивать выполнение основных контрольных процедур до загрузки операционной системы, т. е. на аппаратном уровне. При этом контроль целостности системных областей и файлов, данных и процедур должен осуществляться устойчивым к воздействиям механизмом, основанным на применении хэш-функций. На базе этих средств, а также контроля запуска задач должна обеспечиваться корректная поддержка изолированности программной среды.

3. Спектр выпускаемых на аттестованном производстве СЗИ должен перекрывать проблемы защиты в гетерогенных сетях, основанных на интеграции наиболее популярных ОС, в том числе MS DOS, Novell Net Ware, Windows 3.11, Windows 95 и последующие модели, Windows NT. Корректная работа в данных средах может основываться только на принципах операционной независимости программных средств СЗИ и транспортного механизма, не зависящего от типа сетевой ОС.

4. Состав атрибутов, на основе которых описываются правила разграничения доступа (ПРД) к объектам информационной системы, должен быть таким, чтобы обеспечить возможность описания любой разумной непротиворечивой политики безопасности. При этом СЗИ не должна создавать трудностей для пользователей системы — не ограничивать функциональных возможностей, предоставляемых операционной системой, быть «прозрачной» в пределах политики

безопасности для легального пользователя, аутентифицированного защитным механизмом.

5. Для применения в сетевых решениях обязательным является наличие средств централизованного управления безопасностью и средств аудита, в том числе в режиме on line. Средства аутентификации при этом должны обеспечивать не только аутентификацию операторов, но и технических средств комплекса.

6. Обеспечивая целостность и доступность информации, защиту её от несанкционированных модификаций, СЗИ должна предоставлять возможность работы с сертифицированными криптографическими средствами. Важным при этом является отсутствие скрытых (не документированных) возможностей, а также «опасных» реакций на действия операторов.

7. Иметь сертификат в системе сертификации средств защиты информации для класса не ниже 1В и выпускаться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере. Производство технических и программных средств СЗИ должно быть аттестовано и подвергаться периодическому контролю.

5.5.1. Архитектура семейства программно-технических устройств аппаратной защиты информации

Показано, что для аппаратной аутентификации в электронной среде минимальная конфигурация СЗИ должна включать в свой состав следующие функциональные узлы (Рис. 5.1). В энергонезависимой памяти, ЭНП, хранится как минимум эталонная информация для процедур идентификации / аутентификации пользователя, ссылки на полномочия пользователя и контрольные суммы для контроля целостности системных областей и системных файлов. Из ТМИ в контроллер поступает

информация о пользователе и (в общем случае) контрольная сумма прикладных задач и данных. В ЭНП хранится (как минимум) эталонная информация для процедур аутентификации пользователя, ссылки на полномочия пользователя и контрольные суммы для контроля целостности системных областей и системных файлов. Датчик случайных чисел используется как генератор необходимых ключей взаимодействия. ROM BIOS содержит фиксированное описание процедур и преобразований, обеспечивающих все вышеуказанные функции.

В таком случае, в предположении, что нарушитель является легальным пользователем АС, рассмотрим возможную логику действий по подготовке разрушающего программного воздействия (РПВ).

Введем множество пользователей системы $i=\overline{1,m}$, $U = \{U_i\}_{i=1}^{m}$, $|U| = m$, и множество прав пользователей R, $|R| = p$, т.е. $R = \{r_1, r_2, \ldots, r_p\}$. Рассмотрим подмножество $R_H \subseteq R$, $|R_H| = p_H$, содержащее элементы $r_{H1}, \mathbf{K}, r_{Hp_H}$, а также подмножества вида $R_i \subseteq R$, $|R_i| = p_i$, $\{r_{i1}, \mathbf{K}, r_{ip_i}\} \in R$. Тогда определим множество всевозможных подмножеств R_i множества R: $R_i \in \{R_i\}_{i=1}^{m}$. Элементы этого множества есть права доступа пользователей системы $U_i \in U$.

В ЭНП для i-ого пользователя зафиксирована $\{I_i, P_i, G_i, R_i\}$, где: I_i — идентификатор пользователя i, U_i, $I_i \in \{I_i\}_{i=1}^{m}$; P_i — пароль пользователя i U_i; G_i — контрольная сумма i, $G_i \in \{G_i\}_{i=1}^{m}$; R_i — права пользователя i U_i, $R_i \in \{R_i\}_{i=1}^{m}$. В ТМ, принадлежащей пользователю U_i, при этом хранится пара $\{I_i, G_i\}$.

С учетом особенностей потоков информации между узлами устройства определены основные параметры архитектуры семейства программно-технических устройств защиты информации.

Как отмечалось выше, на ТМ должна храниться не только идентифицирующая пользователя информация, но и отчуждаемые данные для аутентификации и контроля целостности, ключи шифрования (или их части). Утечка (перехват) этих данных может привести к дискредитации защиты. Действительно, так как изменение данных в компьютере может сопровождаться изменениями данных в ТМ, контроллер должен обеспечивать и чтение, и запись. При этом логика действий нарушителя, в предположении, что нарушитель является легальным пользователем АС, могла бы быть такой: подготовить разрушающее программное воздействие (РПВ), выполняющее следующие функции:

а) фиксируются тройки $\{I_i, P_i, G_i\}$ и соответствующие им права R_i при легальном входе пользователей за период времени T;

б) анализируется информация о правах $\{R_l\}_{l=1}^{k} \subset \{R_i\}_{i=1}^{m}$, где $k \le m$, k – число различных пользователей, зафиксированных РПВ, и выбирается в качестве прав, которые необходимы нарушителю;

в) при загрузке нарушителем $U_н$ с $\{I_н, P_н, G_н\}$ эта совокупность заменяется на $\{I_j, P_j, G_j\}$, что позволяет пользователю $U_н$ получить права R_j.

Принципиальная осуществимость атак такого рода возможна лишь потому, что:

а) носящие конфиденциальный характер данные попадают в оперативную память ЭВМ, где к ним может получить доступ РПВ;

б) обработка данных выполняется процессором ЭВМ, который не различает источника данных. Отсюда следует возможность подмены данных.

Очевидно, что для того, чтобы противостоять атакам этого типа, необходимо изменить архитектуру контроллера — организовать каналы передачи данных, минуя RAM ЭВМ, и ввести микропроцессорное устройство управления (MCU), на основе которого будет осуществляться

обработка данных, носящих конфиденциальный характер. В этом случае примерная структура контроллера может выглядеть так, как показано на рис. 5.3. В принципе, такое устройство вполне работоспособно, и на практике остается лишь рассмотреть особенности связей и функциональность MCU с целью дооснащения устройства дополнительными блоками.

Важнейшей особенностью любого устройства является адаптивность. Так, например, до сих пор не существует стандарта на шину ISA — стало быть, вероятна необходимость адаптации ИВВ. Дополнение котроллера функциональными блоками может привести к изменению ПО MCU. Это означает, что функциональность основных узлов контроллера должна определяться уже после изготовления контроллера путем программирования с использованием специализированного программатора, который должен входить в состав контроллера.

Для того чтобы снять ограничения по подключению к контроллеру дополнительных устройств, целесообразно использовать магистрально-модульный принцип организации вычислительных устройств. При этом полезно организовать поддержку наиболее применимых интерфейсов и шин, и в дальнейшем их можно будет использовать для расширения функциональных возможностей устройства. Такими шинами и интерфейсами могли бы быть RS232C, I^2C, SPI. С точки зрения дополнительных устройств структура устройства может быть такой, как показано на рис. 5.4. Рассматривая этот вариант архитектуры, нетрудно заметить присутствующие противоречия. Программное обеспечение, записанное в ROM BIOS, с одной стороны, не должно меняться для гарантированности стабильности свойств, но возможность его модификации должна быть предусмотрена для обеспечения адаптивности. Это же касается и других программируемых узлов устройства. Данное

противоречие может быть разрешено путем введения двух режимов функционирования устройства:

- рабочего, в котором функциональность исполняется, но модификации невозможны;
- специального (технологического), в котором исполняются только функции программирования узлов устройства.

Переход от одного к другому режиму должен реализовываться физическими (контролируемыми), а не программными методами.

5.5.2. Аппаратный модуль доверенной загрузки (АМДЗ)

Такая структура СЗИ позволяет реализовывать все функции аппаратного модуля доверенной загрузки (АМДЗ) с возможностью применения его в качестве резидентного компонента безопасности — РКБ [76, 78—79]. АМДЗ определяется как средство, обеспечивающее доверенную загрузку ОС вне зависимости от ее типа для аутентифицированного защитным механизмов пользователя (Рис. 5.5). Основными функциями АМДЗ являются: администрирование; идентификация и аутентификация; пошаговый механизм контроля целостности для FAT, NTFS, HPFS, FreeBSd и др.; выработка кодов аутентификации; коммутация физических линий; хранение и применение ключей; управление доступом к логическим дискам. Его отличительными особенностями являются:

- модульная архитектура со спецканалами;
- программируемость всех узлов (ISP-технология);
- возможность расширения путем подключения дополнительного оборудования по стандартным каналам;
- функциональная достаточность резидентного ПО.

Аппаратный модуль доверенной загрузки (АМДЗ) предназначен для работы в IBM PC совместимых компьютерах, имеющих слоты плат расширения ISA (XT или AT), или PCI в составе программно-аппаратных комплексов защиты информации от несанкционированного доступа. Плата контроллера выполнена как полностью программируемое устройство (In-System-Programmable — ISP) (Рис. 5.6). Функциональное назначение контроллера определяется программированием его составных частей:

- интерфейса шины (BusInt);
- постоянного запоминающего устройства типа Flash (ROM);
- микроконтроллера (MCU).

Программирование и модификация BusInt производится в **технологическом** режиме, а ROM и MCU — в **специальном**. Конструкция контроллера обеспечивает его работу в этих режимах только при вскрытии корпуса компьютера, извлечения платы из слота motherboard и отсоединения крепежного кронштейна, что служит защитой от проведения такой операции несанкционированно или случайно. Контроллер при подсоединении специального программатора, работающего под управлением IBM PC совместимого компьютера, переходит в технологический режим, который обеспечивает программирование интерфейса. Возможность перепрограммирования блокируется при установке платы в слот расширения ЭВМ и/или при установке крепежного кронштейна.

Рассмотрены особенности реализации следующих функциональных блоков АМДЗ.

Интерфейс шины контроллера обеспечивает доступ центрального процессора ЭВМ к ROM и MCU. Конструкция программируемых микросхем BusInt и MCU обеспечивает защиту от модификации и чтения записанной в них информации в любом режиме. Программатор MCU доступен только в специальном режиме.

Адресная селекция и контроль — доступ к ROM, программирование ROM (для программирования ROM контроллер должен работать в специальном режиме, возможность перепрограммирования ROM блокируется при установке крепежного кронштейна).

Интерфейс с MCU доступен в специальном и обычном режимах. MCU работает под управлением собственного встроенного ПО и выполняет функцию «электронного замка» для доступа пользователей к таким ресурсам как:

- вычислительные функции микроконтроллера;
- встроенная энергонезависимая память микроконтроллера (EEPROM);
- энергонезависимая память большого объема (DataFlash);
- внешний интерфейс (TM или RS-232);
- датчик случайных чисел;
- возможность физического отключения устройств;
- расширение интерфейса SPI.

Дополнительные устройства подключается к спецканалам, которые, в свою очередь, управляются MCU. Рассмотрены часто применяемые дополнительные устройства, такие, как ДСЧ, энергонезависимая память, блок контроля физических линий, батареечные устройства (БатУ).

- **Датчик случайных чисел — ДСЧ**. Микроконтроллер по запросу CPU может сформировать байт случайного числа, получаемого с помощью шумовых диодов. Наличие у микроконтроллера аналогового компаратора позволяет использовать две схемы ДСЧ — спецификации R и K.
- **TM интерфейс RS-232**. Микроконтроллер может поддерживать функцию однопроводного (One Wire) интерфейса, предназначенного

для подключения фирмы Dallas, или интерфейса RS-232 для подключения стандартных устройств.

- **Энергонезависимая память Data Flash**. Микроконтроллер через интерфейс SPI подключен к энергонезависимой памяти (Serial EEPROM) объемом до 1 Мбит, что позволяет создавать пользовательские архивы.
- **Контроль физических линий**. Микроконтроллер управляет двумя реле, которые могут быть использованы для физического подключения/ подключения/отключения (коммутированная на землю или питание) управляющих цепей внешних устройств.
- **Батареечные устройства — БатУ.** Особенности БатУ заключаются в том, что с их помощью можно организовать аудит тех событий, которые ранее были неконтролируемы. Так, например, БатУ позволяет в своей памяти фиксировать вскрытие корпуса и изъятие платы контроллера (в том числе для выключенного компьютера). В памяти могут фиксироваться также события, связанные с аудитом администратора.

Функциональность АМДЗ обеспечивается программированием MCU контроллера. Рассмотрены особенности программирования АМДЗ с учетом режима его работы и особенностей реализации контрольных функций. MCU содержит два программируемых блока — память программ и энергонезависимую память данных (EEPROM). Конструкция микросхемы MCU обеспечивает защиту от модификации и чтения в любом режиме как собственно его программы, так содержимого EEPROM.

Другими словами, программа MCU и данные в EEPROM, как записанные пользователем в **специальном** режиме, так и сформированные в процессе функционирования контроллера в **рабочем** режиме, могут быть только уничтожены, но не изменены или считаны. И только после стирания содержимого памяти программ и EEPROM, MCU можно снова

запрограммировать в **специальном** режиме. Возможность перепрограммирования MCU блокируется при установке крепежного кронштейна.

5.6. Выводы

1. Показано различие между идентификацией и аутентификацией и дано определение аутентификации. Идентификация объекта — это установление (отношения) эквивалентности между объектом и его априорным обозначением (определением, представлением, образом, комплексом характеристик и т. п.).

Аутентификация ***причастного к документу*** *объекта или процесса (автора, отправителя, получателя, оператора, процедуры, технологии и пр.) — это* ***объективное*** *подтверждение содержащейся в документе* ***идентифицирующей*** *информации об этом объекте или процессе.*

2. Традиционно задачи аутентификации и классификации определяются на разном предметном поле: в первой — одному документу x необходимо поставить в соответствие единственный объект (например, автора) y; во второй — *множество* объектов $x \in X$ разбивается на *множество* классов $y \in Y$. Установлено, что аутентификация данного документа x возможна, если и только если возможна классификация множества X документов, в которое входит аутентифицируемый документ x. Без описания множеств объектов X и классов Y классификация и, следовательно, аутентификация невозможны.

Документ d отображается в виде пары чисел $d = \langle x, i \rangle$, где x — содержание документа (текст), $i = i(x)$ — признак эквивалентности класса (идентификатор). *Аутентификация сводится к классификации* пары $d = \langle x, i \rangle$ на основании идентификатора $i = i(x)$. При единственном

признаке эквивалентности $i(x)$ можно говорить об одномерной классификации, при нескольких — о многомерной. Формально многомерная классификация всегда сводится к одномерной.

3. В системе «пространство-время» точка «0» формирования ЭлД и точка «1» его аутентификации различны. На этапе жизненного цикла ЭлД между точками «0» и «1» в агрессивной электронной среде возможна подделка, следовательно, каждому документу $d = \langle x, i \rangle$ в точке «0» соответствует в точке «1» подмножество $d \cup \bar{d}$ множества $X_1 = X \cup \bar{X}$, где $\bar{X}$ — подмножество «поддельных» документов, порожденных документом d и отличающихся от него либо текстом $\bar{x}$, либо идентификатором $\bar{i}$, либо тем и другим.

В точке аутентификации наблюдаемое множество X_1 предварительно надо разделить на классы X и $\bar{X}$ — приходим к двухмерной классификации. Нужен дополнительный признак эквивалентности h, поэтому формируемый в точке «0» документ должен представлять собой трио $d = \langle x, i, h \rangle$, где $h = h(x, i)$, или $h = h_i(x)$, или $h = h_x(i)$. Если возможно согласованное искажение всех элементов трио $\langle x, i, h \rangle$, то ЭлД должен формироваться в виде квартета $d = \langle x, i, h, p \rangle$, где p — индикатор некой криптографии, связывающей элементы трио $\langle x, i, h \rangle$.

4. Механизмы аутентификации делятся на два класса: построенные на основе асимметричных методов — электронная цифровая подпись, ЭЦП; на основе симметричных методов — защитный код аутентификации, ЗКА. Анализ наиболее распространенных архитектур электронного взаимодействия: «каждый с каждым», последовательная, распределенная сеть, радиальная (звезда), иерархическая (дерево), показывает, что, за исключением системы «каждый с каждым», все остальные характеризуются сопоставимыми объемами хранимой защищаемой информации как при использовании ЭЦП, так и ЗКА.

Трудоемкость и требуемые ресурсы для применения ЗКА на несколько порядков меньше ресурсов, требуемых для применения ЭЦП, что позволяет реализовать аутентификацию ЭлД *вне* основной среды вычислений — в рамках специализированных контроллеров.

5. Применение для аутентификации ЗКА предпочтительно, если одновременно выполняются следующие условия: юридическая ответственность за нарушение тайны ключей аутентификации невозможна (электронная среда) или нецелесообразна (административные методы эффективнее); архитектура электронного взаимодействия обеспечивает сопоставимый объем хранимой секретной информации о ключах аутентификации. Как правило, эти условия выполняются в вычислительных системах централизованных корпораций и фирм. Необходимо разумное сочетание механизмов аутентификации: ЭЦП — на «внешних» сечениях ВС; ЗКА — на «внутренних».

6. Исходя из установленных положений, показано, что для аппаратной аутентификации в электронной среде минимальная конфигурация соответствующего резидентного компонента безопасности (РКБ) должна включать в свой состав следующие функциональные узлы:

- touch-memory интерфейс — ТМИ;
- энергонезависимую память — ЭНП;
- датчик случайных чисел — ДСЧ;
- постоянное запоминающее устройство (ПЗУ) пользовательского расширения BIOS — ROM BIOS;
- интерфейс связи с ЭВМ — ИВВ.

Аппаратная реализация в силу физической изолированности обеспечивает эффективную защиту от НСД наиболее важных процедур и данных, используемых при аутентификации ЭлД. Но в любом случае взаимодействие с вычислительной средой, окружающей РКБ, необходимо

должно существовать. Соответственно, предусматривается интерфейс связи с ЭВМ — ИВВ (интерфейс ввода-вывода).

7. Функциональные возможности средств защиты информации (СЗИ) должны обеспечивать выполнение основных контрольных процедур *до загрузки операционной системы*, т. е. на аппаратном уровне. При этом контроль целостности системных областей и файлов, данных и процедур должен осуществляться устойчивым к воздействиям механизмом, основанным на применении хэш-функций. На базе этих средств, а также контроля запуска задач должна обеспечиваться корректная поддержка изолированности программной среды. Сформулированы основные требования к функциональности и составу аппаратных средств защиты информации (СЗИ).

8. В предположении, что нарушитель является легальным пользователем АС, рассматривается наиболее распространенный вариант подготовки разрушающего программного воздействия (РПВ). Чтобы противостоять атакам этого типа, необходимо усовершенствовать архитектуру контроллера — организовать каналы передачи данных, минуя RAM ЭВМ, и ввести микропроцессорное устройство управления (MCU), на котором будет осуществляться обработка данных, носящих конфиденциальный характер. Функциональность основных узлов контроллера должна определяться уже после изготовления контроллера путем программирования с использованием специализированного программатора, который должен входить в состав контроллера.

9. Программное обеспечение, записанное в ROM BIOS, с одной стороны, не должно меняться для гарантированности стабильности свойств, но возможность его модификации должна быть предусмотрена для обеспечения адаптивности. Это же касается и других программируемых узлов устройства. Данное противоречие разрешено путем введения двух режимов функционирования устройства:

- рабочего, в котором функциональность исполняется, но модификации невозможны;
- специального, в котором исполняются только функции программирования узлов устройства.

Переход от одного к другому режиму должен реализовываться физическими (контролируемыми), а не программными методами.

10. Аппаратный модуль доверенной загрузки (АМДЗ) есть средство, обеспечивающее доверенную загрузку ОС вне зависимости от ее типа для аутентифицированного защитным механизмом пользователя. Плата контроллера выполнена как полностью программируемое устройство — ISP. Функциональное назначение контроллера определяется программированием его составных частей: интерфейса шины (BusInt); постоянного запоминающего устройства типа Flash (ROM); микроконтроллера (MCU). Программирование и модификация BusInt производится в технологическом режиме, а ROM и MCU — в специальном. Рассмотрены особенности программирования АМДЗ с учетом режима его работы и особенностей реализации контрольных функций, рассмотрены функции и задачи отдельных устройств.

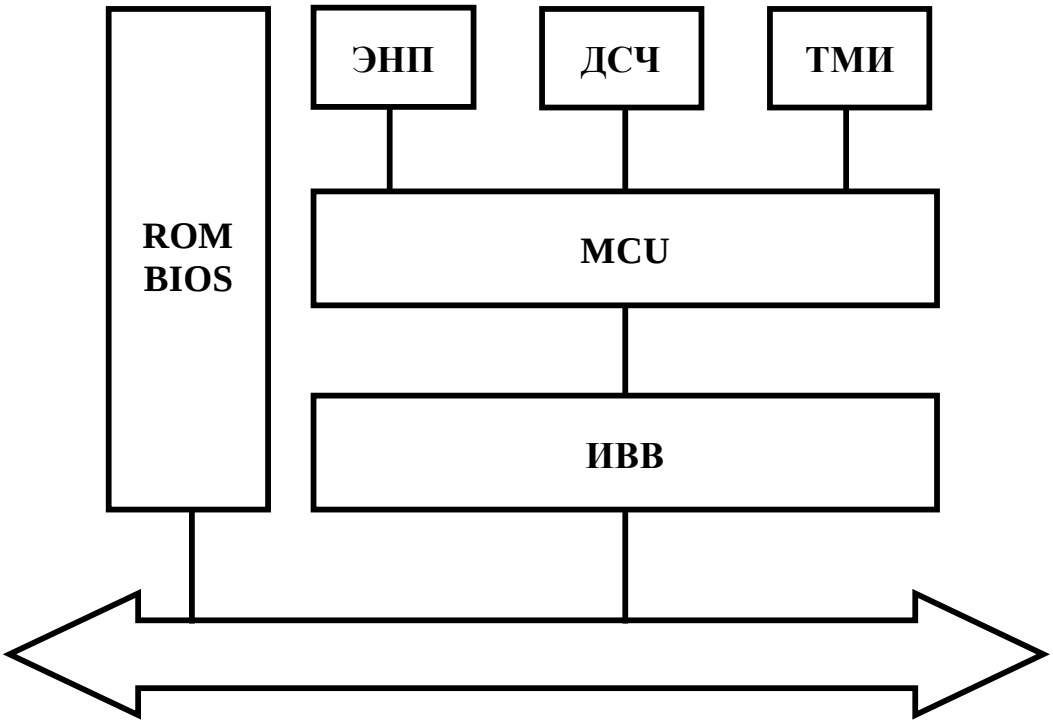


Рис. 5.3. Блок-схема построения резидентного компонента безопасности (MCU — микропроцессорное устройство управления; ЭНП — энерго–независимая память; ДСЧ — датчик случайных чисел; ТМИ — touch–memory интерфейс; ИВВ — интерфейс связи с ЭВМ)

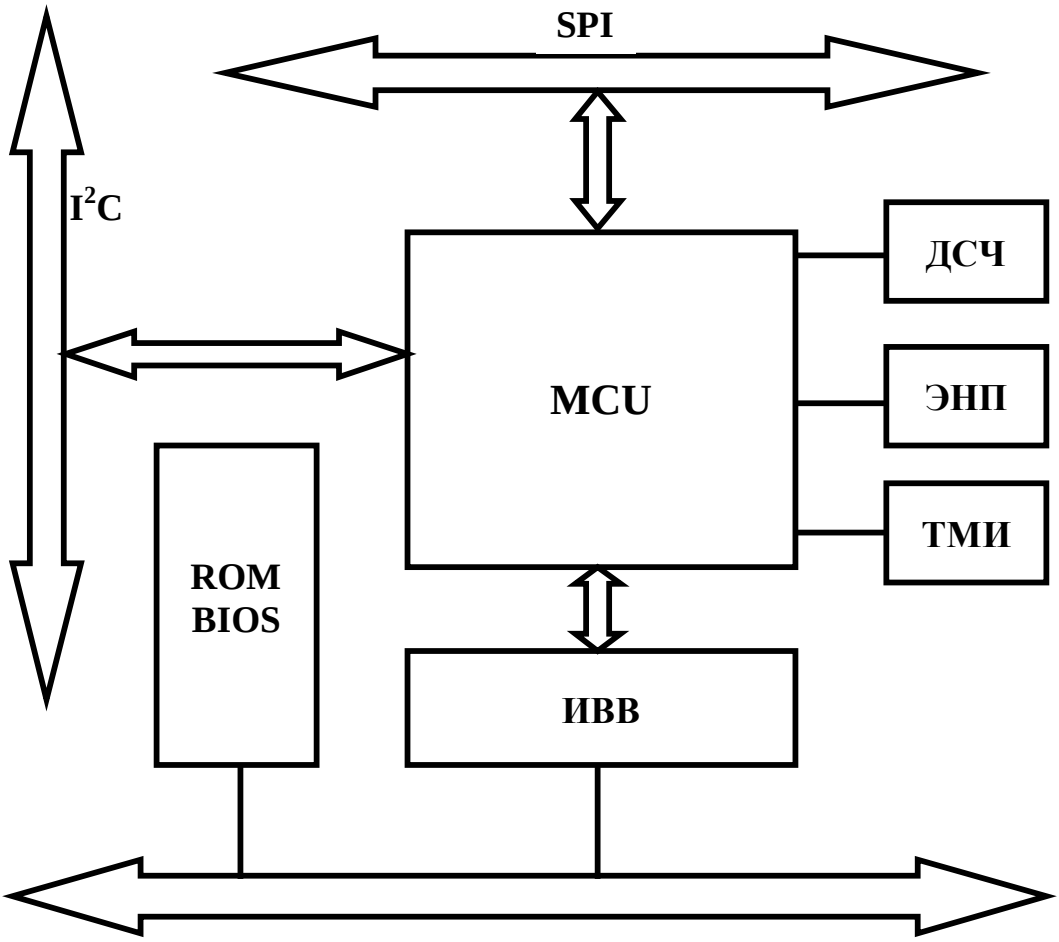


Рис. 5.4. Архитектура резидентного компонента безопасности

Рис. 5.5. Задачи аппаратного модуля доверенной загрузки — АМДЗ

Рис. 5.6. Функции аппаратного модуля доверенной загрузки — АМДЗ

ЛИТЕРАТУРА

1. Кузнецов Н. А., Мусхелишвили Н. Л., Шрейдер Ю. А. Информационное взаимодействие как объект научного исследования (перспективы информатики) // Вопросы философии. № 1. 1999. С. 77–87.
2. Шеннон К. Работы по теории информации и кибернетике. М., 1963.
3. Колмогоров А. Н. Три подхода к определению понятия «Количество информации» // Новое в жизни, науке, технике. Сер. «Математика, кибернетика». № 1. 1991. С. 24–29.
4. Гоппа В. Д. Введение в алгебраическую теорию информации. М., 1995.
5. Винер Н. Кибернетика или управление и связь в животном и машине. 2-е изд. М., 1968. С. 201.
6. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М., 1996.
7. Большой юридический словарь / Под ред. А. Я. Сухарева, В. Е. Крутских. М., 2000.
8. Гадасин В. А., Конявский В. А. От документа — к электронному документу. Системные основы. М., 2001.
9. Гадасин В. А. Закон и электронный документооборот. Можно ли законы применять на практике // Connect! Мир связи. № 2. 2002. С. 26–29; № 3. 2002. С. 64–66.
10. Гадасин В. А., Конявский В. А. Так жить нельзя. Существует формально такое понятие как электронная информация? // Форум IT. № 1(01). Октябрь/Ноябрь. 2002. С. 24–26.
11. Гадасин В. А. Общая оценка законодательной базы в сфере электронного документооборота // Управление защитой информации. Т.6. № 2. 2002. С. 117–121.
12. Конявский В. А., Гадасин В. А. Системное различие традиционного и электронного документов // Безопасность информационных технологий. № 3. 2001. С. 39–51.
13. Трахтенброт Б. А. Алгоритмы и вычислительные автоматы. М., 1974.
14. Кузнецов Н. А., Полонников Р. И., Юсупов Р. М. Состояние, перспективы и проблемы развития информатики // Проблемы информатизации. Вып. 1. 2000. С. 5–12.
15. Проект Федерального закона «Об электронной цифровой подписи» (от 15.05.2000 г.) // Управление защитой информации. Т.4. № 4. 2000. С. 477–484.
16. Проект Закона Республики Казахстан «Об электронном документе и электронной цифровой подписи».
17. Проект Федерального закона «О предоставлении электронных услуг» (от 21.07.2000 г.)
18. Проект Федерального закона «Об информации, информатизации, и защите информации» // Управление защитой информации. Т.4. № 2. 2000. С. 163–170.
19. Проект Федерального закона «Об электронной торговле» (от 02.10.2000 г.)

20. Проект Федерального закона «Об электронной цифровой подписи» // Безопасность информационных технологий. № 2. 2000. С. 100–106.
21. Проект Федерального закона «Об электронном документе» (от 20.03.2001 г.)
22. Федеральный закон «О библиотечном деле» (от 29.12.1994 г.) // СЗ РФ (Собрание законодательства Российской Федерации). 1995. № 1. Ст. 2.
23. Федеральный закон «Об информации, информатизации и защите информации» (от 20.02.1995 г.) // СЗ РФ. 1995. № 8. Ст. 609.
24. Федеральный закон «Об обязательном экземпляре документов» (от 29.12.1994 г.) // СЗ РФ. 1995. № 1. Ст. 1.
25. Федеральный закон «Об участии в международном информационном обмене» (от 04.07.1996 г.) // СЗ РФ. 1996. № 28. Ст. 3347.
26. Федеральный закон «Об электронной цифровой подписи» (от 10.01.2002 г.) // Российская газета, январь 2002 г.
27. ГОСТ ИСО/МЭК 2382–01–99 (Проект). «Межгосударственный стандарт. Информационная технология. Словарь. Часть 01. Основные термины». М.: Госстандарт России, 1999.
28. ГОСТ Р ИСО/МЭК 9594-8-98 «Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации». М.: Госстандарт России, 1998.
29. Международный стандарт ИСО/МЭК 14888-1-98 «Информационная технология. Методы защиты. Цифровые подписи с приложением».
30. ГОСТ Р 51141 – 98. «Делопроизводство и архивное дело. Термины и определения». М.: Госстандарт России, 1998.
31. ГОСТ Р 6.30—97. «Унифицированные системы документации. Унифицированная система организационно–распорядительной документации. Требования к оформлению документов». М.: Госстандарт России, 1997.
32. Закон Верховного Совета Республики Хакасии «Об информации, информатизации и защите информации в Республике Хакасия» (от 19.10.1999 г., № 65).
33. Закон Республики Беларусь «Об электронном документе» (от 10. 01. 2000 г., № 357–З) // Управление защитой информации. Т. 4. № 1. 2000. С. 60–65.
34. Закон РФ «О государственной тайне» (от 21.07.1993 г. в редакции от 06.10.97 г.) // Российская газета. 1997. 9 окт.
35. Закон РФ «Об авторском праве и смежных правах» (от 19.07.1995 г.) // СЗ РФ. 1995. № 30. Ст. 2866.
36. Закон Туркменистана «Об электронном документе» (от 19.12.2000 г.).
37. Общероссийский классификатор управленческой документации. ОК 011–93. М.: ИПК Издательство Стандартов, 1999.
38. ГОСТ Р 34.10.94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».
39. Грунтович М. М. О «двуличии» в алгоритмах цифровой подписи // Управление защитой информации. Т. 6. № 2. 2002. С. 55–58.

40. Шеннон К. Математическая теория связи // Работы по теории информации и кибернетике. М., 1963. С. 243–332.
41. Устинов Г. Н. Основы информационной безопасности систем и сетей передачи данных. М., 2000.
42. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа и информации. Показатели защищенности от несанкционированного доступа к информации. М.: Военное издательство, 1992.
43. Зегжда П. Д., Зегжда Д. П., Семьянов П. В. и др. Теория и практика обеспечения информационной безопасности. М., 1996.
44. Хоффман Л. Дж. Современные методы защиты информации. М., 1980.
45. Harrison M. A., Ruzzo W. L. Security Specifications // IEEE Symposium on Security and Privacy. Oakland, 1988.
46. Ухлинов Л. М. Управление безопасностью информации в автоматизированных системах. М., 1996.
47. Bell D. E., La Padulla J. Security Computer System: A Mathematical Model. Bedford, Massachusetts: Mitre Corp., 1973. № 11.
48. Landwerh C., Heitmeyer C., McLean J. A security model for militery message. ACM Trasactions on Computer System, 1984. V.2. № 3.
49. Shandhu R. Transformation of access right // IEEE Symposium on Security and Privacy. Oakland, 1989.
50. Shandhu R. The Schematic Protection Model: It's Definition and Anlisis for Acyclic Attenuating Schem. Journal of ACM 1988. V.35. № 2.
51. Benson G., Appelbe W., Akyldiz I. The hierarhicical model of distributed system security // IEEE Symposium on Security and Privacy. Oakland, 1989.
52. Jeremy J. Security Specifications // IEEE Symposium on Security and Privacy. Oakland, 1988.
53. Wisoman S., Terry D. A new security policy mode // IEEE Symposium on Security and Privacy. Oakland, 1989.
54. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997.
55. Clements D., Hoffman L. J. Computer Assisted Security System Design. ERL Memo M-468, Electronics Research Laboratory, University of California, Berkeley, Nov. 1974.
56. Абрамов В. А. Введение в теорию систем детерминированного, стохастического и нечеткого типа. М., 1980.
57. Zadeh L. A. The Concept of a Linguistic Variable and Its Application to Approximate Reasoning. Memo ERL-M411, Electronics Research Laboratory, University of California, Berkeley, Oct. 15, 1973.
58. Прокофьев И. В. Шрамков И. Г. Щербаков А. Ю. Введение в теоретические основы компьютерной безопасности. М., 1998.
59. Щербаков А. Ю. Методы и модели проектирования средств обеспечения безопасности в распределенных компьютерных системах на основе создания изолированной программной среды. Автореф. дис. … д-ра техн. наук. М., 1997.

60. Программно-аппаратный комплекс защиты компьютера от несанкционированного доступа Dallas Lock 4.0. Конфидент. СПб., 1997.
61. Система разграничения доступа Secret Net v.1.10. Руководство. SafeWare Group.
62. Аккорд 1.95. Описание применения. 1143195.4012-003 31. ОКБ САПР. М., 1997.
63. McLean J. Reasoning About Security Models, Proceedings, IEEE Symposium on Privacy and Security, Oakland, CA April 1987, IEEE Computer Society Press, 1987.
64. Гадасин В. А., Конявский В. А. Системные понятия электронного взаимодействия // Безопасность информационных технологий. № 3. 2002. С. 39–48.
65. Кац М., Улам С. Математика и логика. Ретроспектива и перспективы. М., 1971.
66. Жельников В. Криптография от папируса до компьютера. М., 1997.
67. Колмогоров А. Н., Фомин С. В. Теория функций и функционального анализа. М., 1964.
68. Смирнов А., Криворученко И., Криворученко В. Еще раз о системном подходе к формулировкам. Что такое электронные данные, сведения, документы в терминологии информатики // PC Week/RE. № 17. 2000. С. 32.
69. Смирнов А., Криворученко И., Криворученко В. Системный подход к формулированию определений информатики // PC Week/RE. № 18. 1999. С. 16.
70. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. М., 1999.
71. Феллер У. Введение в теорию вероятностей и ее приложения. Т. 1. М., 1964.
72. Ходаковский Е. А. Системология безопасности // Безопасность. Информационный сборник фонда национальной и международной безопасности. № 7–9 (39). 1997. С. 178–185.
73. Руководящие документы. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М., Гостехкомиссия России, 1992.
74. Руководящие документы. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М., Гостехкомиссия, 1997.
75. Кузнецов О. П., Адельсон-Вельский Г. М. Дискретная математика для инженеров. М., 1988.
76. Конявский В. А. Управление защитой информации на базе СЗИ НСД «Аккорд». М., 1999.
77. Конявский В. А. Аккорд – гармония безопасности // Бизнес и безопасность в России. 1996. № 2–3. С. 56.
78. Конявский В. А. Методы и механизмы аппаратной безопасности // Безопасность информационных технологий. 1999. № 1. С. 59–73.
79. Конявский В. А. Аппаратный модуль доверенной загрузки (Аккорд-АМДЗ) // Банковское дело в Москве. 1998. № 4 (40).
80. Волокитин А. В., Маношкин А. П., Солдатенков А. В., Савченко С. А., Петров Ю. А. Информационная безопасность государственных организаций и

коммерческих фирм. Справочное пособие / Под общ. ред. Л. Д. Реймана. М., 2002.

81. Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В. А. Садовничего, В. П. Шерстюка. М., 2002.
82. Конявский В. А. Основные направления обеспечения информационной безопасности в информационных системах и сетях // Управление защитой информации. Т.5. № 2. 2001. С. 147–157.
83. Конявский В. А., Жуков Н. С. Техническая защита объектов электросвязи // Электросвязь, 1999. № 9. С. 5–10.
84. Конявский В. А. Основные направления обеспечения информационной безопасности в информационных системах и сетях // Управление защитой информации. Т.5. № 2. 2001. С. 147–157.
85. Закон РФ «О применении контрольно-кассовых машин при осуществлении денежных расчетов с населением» (от 18 июня 1993 г., № 5215-1).
86. Конявский В. А., Малютин А. А. Как выбрать систему защиты от несанкционированного доступа // Банки и технологии. 1996. № 1. С. 57–60.
87. Конявский В. А., Лысенко В. В. О защите информации в ЛВС от НСД из внешней среды // Управление защитой информации. 1998. Т. 2. № 4. С. 320–323.
88. ГОСТ Р 34.11.94 «Информационная технология. Криптографическая защита информации. Функция хэширования».
89. ГОСТ 34.003 – 90 «Информационные технологии. Комплекс стандартов и руководящих документов на автоматизированные системы».