С. В. Запечников

БЕЗОПАСНОСТЬ КЛЮЧЕВЫХ СИСТЕМ СРЕДСТВ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Введение

Важное место среди создаваемых в настоящее время компьютерных информационных систем занимают системы электронного документооборота (ЭДО) в сферах государственного и муниципального управления, образования и здравоохранения, в коммерческой и кредитно-финансовой сферах. В современном понимании системы ЭДО — это не просто средства автоматизации делопроизводства, но комплексные системы информационного обеспечения деятельности организаций, охватывающие весь жизненный цикл документов: создание, редактирование, обработку, доставку заинтересованным лицам, хранение, архивирование, учет и систематизацию.

Одним из самых известных примеров универсальной системы корпоративного ЭДО и планирования деловой деятельности является среда Lotus, разработанная корпорацией IBM, включающая ряд продуктов: сервер Lotus Domino, клиент Lotus Notes, дополнительные серверы для реализации отдельных служб Lotus Sametime, Lotus Activities, средства взаимодействия со средой интеграции корпоративных данных IBM Web Sphere и другими продуктами. Еще одним способом реализации систем ЭДО является применение стандартных средств электронной почты и календарного планирования, таких как Microsoft Outlook, надстраиваемых внешними по отношению к ним прикладными программами. Системы ЭДО нередко интегрируются с системами архивного хранения данных и другими услугами, особенно в рамках усилий по реализации программ «электронного правительства», осуществляемых как у нас в стране, так и за рубежом.

1. Особенности криптографической защиты систем электронного документооборота

С возрастанием количества и расширением масштаба задач, решаемых системами ЭДО, возрастает ответственность за последствия их применения. На одно из первых мест выходит проблема обеспечения безопасности электронных документов, в том числе проблема комплексной защиты информации, обрабатываемой, хранимой и передаваемой в системах ЭДО в условиях критических воздействий: атак злоумышленников, отказов и сбоев технических средств, катастроф, ошибок персонала. Перерывы в функционировании систем ЭДО, ошибочное определение авторства документов, возможность отказа от фактов создания и получения документов способны нанести большой экономический ущерб, привести к расстройству оперативности управления, нанести ущерб чести и достоинству, деловой репутации граждан. Применение средств криптографической защиты, в частности средств шифрования и ЭЦП, является не просто необходимым условием, но единственным средством обеспечения юридической значимости электронных документов, соблюдения законодательства о персональных данных и авторского права. Этим обусловлена необходимость формулирования системы научно обоснованных методов криптографической защиты систем ЭДО, и в том числе методов обеспечения стойкости систем ЭДО к разрушению ключевой системы (КС).

Для решения этой задачи необходимо точно специфицировать состав функций защиты информации, выполняемых системой. В общем случае, как ранее было показано автором в работе [1], выделяются два уровня функций систем ЭДО: единичные информационные взаимодействия субъектов системы (односторонняя передача данных и электронный обмен данными) и процессы деловой деятельности между ними, рассматриваемые в целом. Как правило, для реализации этих функций в системе поддерживаются сервисы доверенной третьей стороны (ДТС).

Любая система защищенного ЭДО реализует некоторое подмножество названных функций посредством симметричных и (или) асимметричных криптосхем. Во втором случае

требуется организация в такой системе процессов управления ключами одним из известных способов: за счет создания инфраструктуры открытых ключей (ИОК), идентификационной либо бессертификатной криптосистемы. На практике преобладает первый способ — ИОК, второй и третий пока рассматриваются как перспективные, хотя попытки создания таких систем ЭДО уже предпринимаются. По этой причине самыми уязвимыми местами системы защищенного ЭДО являются централизованные сервисы: удостоверяющие центры (УЦ), центры генерации ключей, другие сервисы ДТС. Основными источниками угроз для них выступают лица, заинтересованные в подделке юридически значимых документов, вирусные атаки, сбои программного обеспечения и аппаратуры, ошибки персонала.

Предложенный автором в работе [2] метод модельного представления КС средств криптографической защиты информации (СКЗИ) дает удобный способ описания КС продуктов и систем самого разного назначения, в том числе и КС систем защищенного ЭДО. Далее рассмотрим возможные решения по построению систем корпоративного ЭДО с интегрированными в них функциями защиты информации.

2. Защищенный электронный документооборот на основе криптосистем с ИОК

Рассмотрим типовую однодоменную систему защищенного ЭДО с ИОК, предназначенную, например, для внутрикорпоративного ЭДО. Применением методики структурно-параметрического синтеза КС [3] для такой системы ЭДО получается структура КС, показанная на рисунке 1. Структура КС такой системы отличается регулярностью и простотой, что является ее несомненным достоинством с точки зрения стойкости к разрушению ключей.

В целях обеспечения более высоких показателей безопасности ключевого материала УЦ и сервисов ДТС, чем это возможно штатными средствами системы, целесообразно применение схем управления ключевым материалом (СУКМ) [4], например пороговых схем разделения секрета. В частности, секретный ключ УЦ разделяется между группой серверов, взаимодействующих по одноранговой модели. В целях повышения надежности и производительности системы обслуживающие УЦ сервера могут быть объединены в кластер. Для защиты ключей пользователей системы от утраты (компрометации) также возможно применение СУКМ, но таких, которые удобно реализуются на персональных вычислительных средствах с применением дополнительных защищенных носителей информации (интеллектуальных карт, токенов, таблеток «touch memory»), например, схем совершенной опережающей безопасности, схем дистанционного управления ключами.

Для систем с большим количеством пользователей более рациональна многодоменная структура. Она может быть предназначена, например, для организации межведомственного или регионального ЭДО.

Криптосистема с ИОК реализуется во всех современных средах, предназначенных для организации защищенного ЭДО. Вместе с тем такие среды для организации защищенного ЭДО, как IBM Lotus и Microsoft Exchange/Outlook, имеют целый ряд интересных особенностей. Используя тот же способ модельного представления КС [2], можно построить графы, показывающие примерную структуру КС типовых систем защищенного ЭДО на базе этих сред. При этом специфика КС таких систем ЭДО становится особенно хорошо видна. Их структура оказывается существенно сложнее показанной на рисунке 1, что не позволяет показать соответствующие графы в настоящей работе.

3. Защищенный электронный документооборот на основе идентификационных криптосистем

Кроме традиционных криптосистем на базе ИОК, перспективные системы защищенного ЭДО могут строиться на базе идентификационных криптосистем (ИКС).

Идея ИКС впервые высказана А. Шамиром [5]. Схема их функционирования показана на рисунке 2. В криптосистеме с большим числом участников выделяется ДТС, называемая

Центром генерации ключей (ЦГК). Все остальные участники системы могут частично или полностью не доверять друг другу. ЦГК владеет секретным мастер-ключом s, который хранится у него с применением повышенных мер защиты. Дополнительно ЦГК вырабатывает ряд открытых параметров криптосистемы, которые хранятся в специальном небольшом по объему общедоступном справочнике.

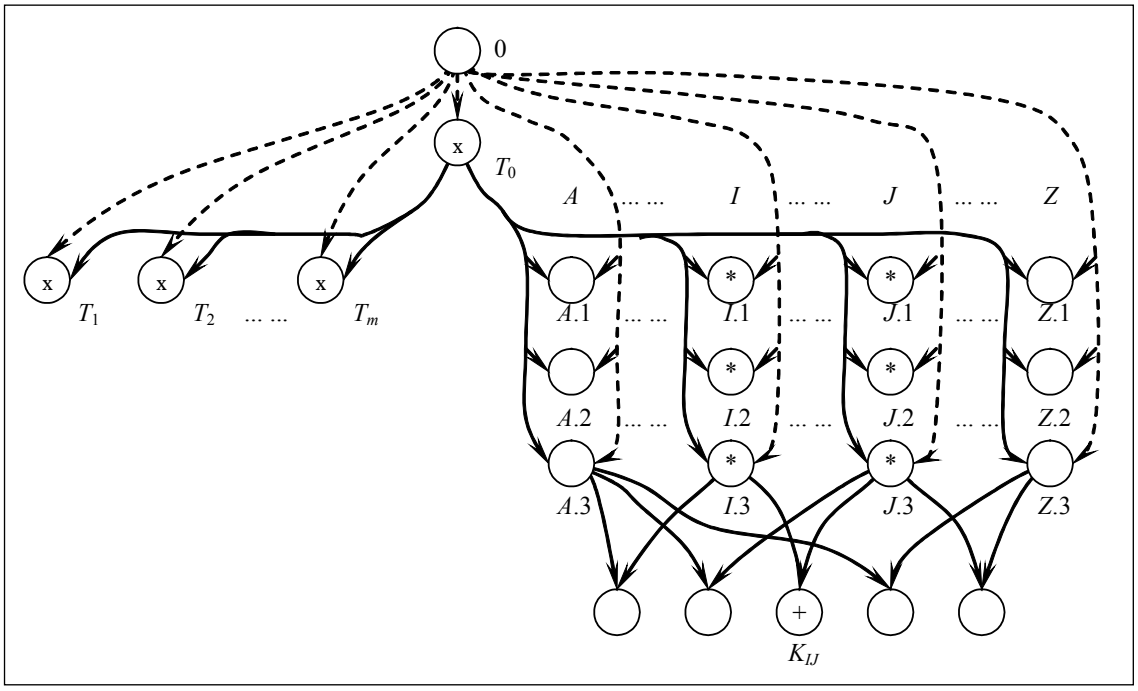

Рис. 1. Структура КС типовой однодоменной системы защищенного ЭДО на основе криптосистемы с ИОК

Обозначения: 0 – ОКС «Параметры криптосистемы»; T_0 – ОКС «Ключи УЦ»; T_1, ..., T_m – ОКС «Ключи ДТС»; A, ..., Z – Участники ЭДО; $A.1$, ..., $Z.1$ – ОКС «Ключи цифровой подписи и сертификат участника ЭДО»; $A.2$, ..., $Z.2$ – ОКС «Ключи открытого шифрования и сертификат участника ЭДО»; $A.3$, ..., $Z.3$ – ОКС «Ключи протокола распределения ключей (ПРК) и сертификат участника ЭДО»; K_{IJ} – ОКС «Общий секретный ключ участников I и J».

Примечание: Для повышения безопасности возможно применение следующих СУКМ: (x) – пороговых схем разделения секрета (СРС) или СРС, функционирующих в модели «проактивной безопасности»; (*) – схем эволюции ключа, обеспечивающих совершенную опережающую безопасность, или резервирования ключей; (+) – схем дистанционного управления ключом.

При введении в систему каждого нового участника — возьмем для примера A — он должен пройти процедуру регистрации в криптосистеме. Для этого он контактирует с ЦГК, чтобы зарегистрировать свой идентификатор и получить от него персональный секретный ключ s_A. Этот ключ вырабатывается ЦГК с помощью некоторой общеизвестной однонаправленной функции f : $s_A = f(ID_A, s)$. ЦГК должен проверить представленные ему учетные данные, а также уникальность идентификатора. Секретный ключ s_A должен быть передан A по защищенному каналу, т. е. для него должна быть обеспечена одновременно конфиденциальность и аутентичность. Идентификатор ID_A общеизвестен (например, адрес электронной почты).

После выполнения всех процедур предварительного этапа такой криптосистемой легко пользоваться. Любому отправителю B, для того чтобы зашифровать сообщение, предназначенное для любого другого участника, не нужно знать ничего, кроме его идентификатора. Например, для отправки сообщения получателю A нужен один лишь его идентификатор ID_A. Расшифровать такое сообщение сможет только тот, кому ЦГК выдал секретный ключ, вычисленный на основе

этого идентификатора, т. е. только A. Принцип устройства ИКС позволяет сделать криптосистему максимально похожей на традиционную систему «бумажной» почтовой связи.

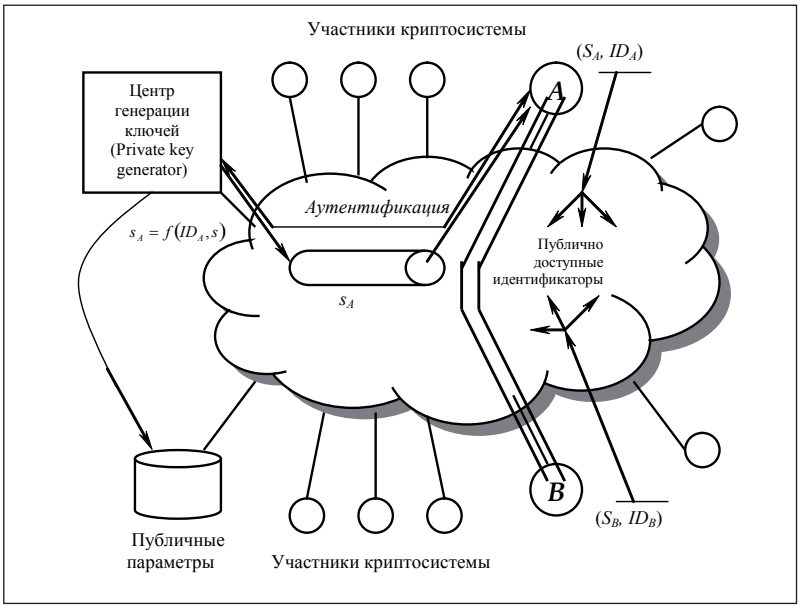

Рис. 2. Схема устройства идентификационной криптосистемы

Главное достоинство ИКС — отсутствие необходимого для ИОК репозитория сертификатов и списков аннулированных сертификатов. Но есть и ряд недостатков: ЦГК знает секретные ключи всех участников криптосистемы; необходима аутентификация участников при регистрации в ЦГК; необходима организация защищенных каналов для передачи секретного ключа от ЦГК к участникам системы; в многодоменной криптосистеме необходима передача публичных параметров ЦГК между доменами, а это дополнительно усложняет протоколы распределения ключей (ПРК).

Все это делает ИКС малопригодными для практического применения в том виде, как они были предложены в [5]. Первая пригодная для практического использования идентификационная криптосхема появилась с разработкой математического аппарата парных отображений: ею стала схема открытого шифрования Боне—Франклина [6], предложенная в 2001 г. Первая идентификационная схема цифровой подписи предложена Боне, Линн и Шачам [7]. Впоследствии в работах различных исследователей было предложено множество криптосхем, предназначенных для работы в ИКС.

В качестве примера можно привести модельную однодоменную систему защищенного ЭДО на основе ИКС. Применением методики структурно-параметрического синтеза КС [3] для такой системы получается структура КС, показанная на рисунке 3.

4. Защищенный электронный документооборот на основе бессертификатных криптосистем

Идея ИКС получила дальнейшее развитие в модели *бессертификатных* криптосистем (БКС), предложенной Аль-Риями и Патерсоном в 2003 г. [8]. Чтобы криптосистема не была полностью зависима от безопасности ЦГК, в ней изменяется процесс генерации секретных ключей участников (Рис. 4).

ЦГК формирует только частичный секретный ключ D_A участника A из секретного мастер-ключа s и идентификатора D_A. Частичный секретный ключ D_A передается от ЦГК к участнику системы по секретному аутентичному каналу связи. Полный секретный ключ S_A формируется как функция персонального секретного ключа k_A участника и частичного секретного ключа D_A, выданного ЦГК. Соответствующий ему открытый ключ P_A формируется как функция персонального секретного ключа k_A участника и общедоступных параметров системы

P^{pub}. Персональный секретный ключ k_A вычисляется как функция от идентификатора D_A и параметров криптосистемы.

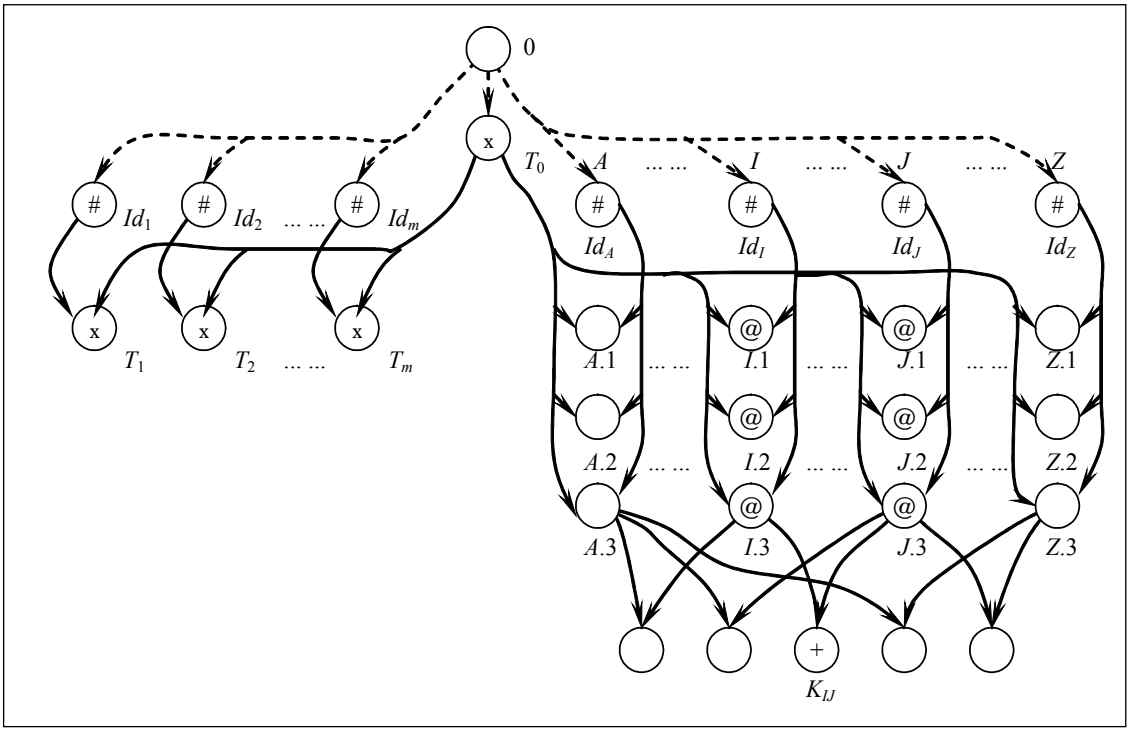

Рис. 3. Структура КС модельной системы защищенного ЭДО на основе ИКС

Обозначения: 0 – ОКС «Параметры криптосистемы»; T_0 – ОКС «Секретный ключ ЦГК»; Id_1, ..., Id_m – ОКС «Идентификаторы ДТС»; T_1, ..., T_m – ОКС «Секретные ключи ДТС»; A, ..., Z – Участники ЭДО; Id_A, ..., Id_Z – ОКС «Идентификаторы участников ЭДО»; $A.1$, ..., $Z.1$ – ОКС «Секретные ключи ЭЦП участника ЭДО»; $A.2$, ..., $Z.2$ – ОКС «Секретные ключи схемы открытого шифрования участника ЭДО»; $A.3$, ..., $Z.3$ – ОКС «Секретные ключи ПРК участника ЭДО»; K_{IJ} – ОКС «Общий секретный ключ участников I и J».

Примечание: Для повышения безопасности возможно применение следующих СУКМ: (x) – пороговых СРС или СРС, функционирующих в модели «проактивной безопасности»; (#) – резервирования ключа; (@) – схем эволюции ключей с изоляцией ключа; (+) – схем дистанционного управления ключом.

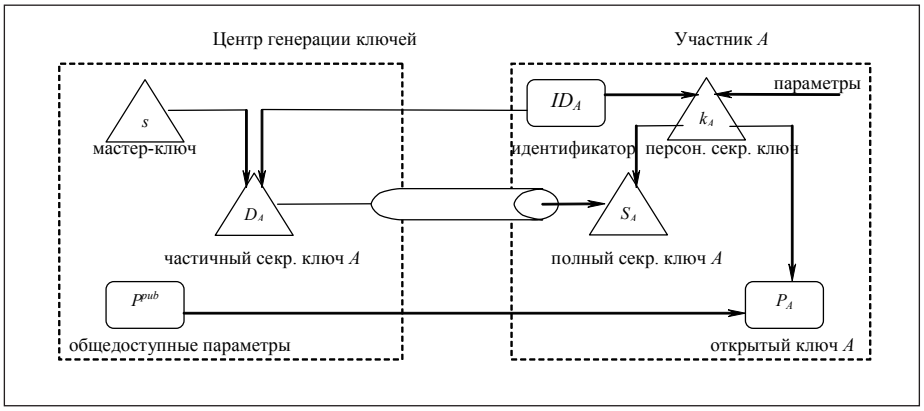

Рис. 4. Схема генерации ключей в бессертификатной криптосистеме

В [9] этот метод был развит: предложена модель ИКС с самогенерирующимися сертификатами. Однако проблема применения всех видов ИКС заключается в том, что для каждой вновь предлагаемой модели устройства криптосистемы необходимо конструирование совершенно новых криптосхем и доказательство их стойкости.

Другим примером служит модельная однодоменная система защищенного ЭДО на основе БКС. Применением той же методики синтеза КС для нее получается структура КС, показанная на рисунке 5.

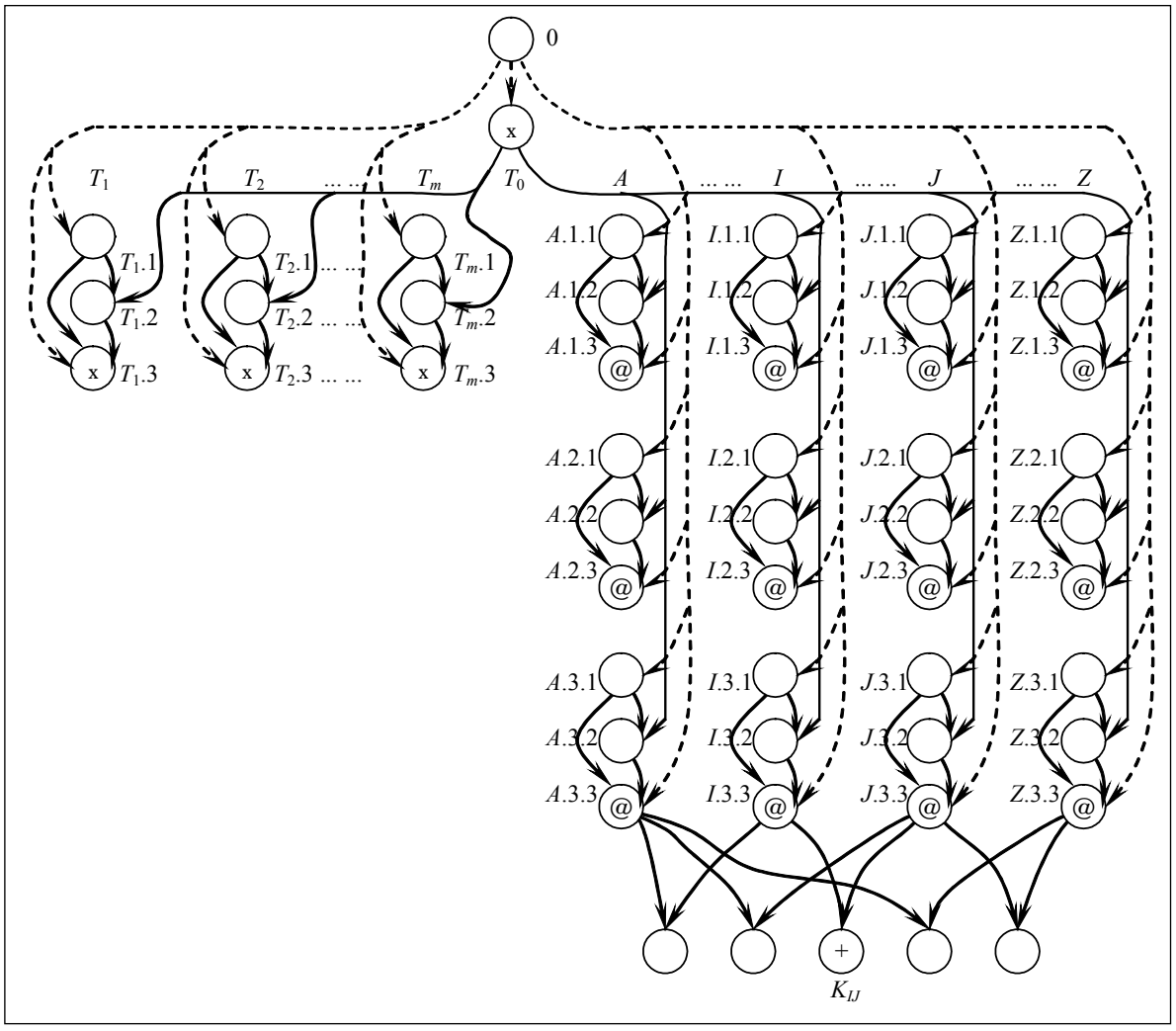

Рис. 5. Структура КС модельной системы защищенного ЭДО на основе БКС

Обозначения: 0 – ОКС «Параметры криптосистемы»; T_0 – ОКС «Ключи ЦГК»; T_1, ..., T_m – Участники системы, выполняющие функции ДТС; $T_1.1$, ..., $T_m.1$ – ОКС «Идентификатор и персональный секретный ключ ДТС»; $T_1.2$, ..., $T_m.2$ – ОКС «Частичный секретный ключ ДТС»; $T_1.3$, ..., $T_m.3$ – ОКС «Полный секретный ключ и открытый ключ ДТС»; A, ..., Z – Участники ЭДО; $A.1.1$, ..., $Z.1.1$ – ОКС «Идентификатор и персональный секретный ключ ЭЦП участника ЭДО»; $A.1.2$, ..., $Z.1.2$ – ОКС «Частичный секретный ключ ЭЦП участника ЭДО»; $A.1.3$, ..., $Z.1.3$ – ОКС «Полный секретный ключ и открытый ключ ЭЦП участника ЭДО»; $A.2.1$, ..., $Z.2.1$ – ОКС «Идентификатор и персональный секретный ключ схемы открытого шифрования участника ЭДО»; $A.2.2$, ..., $Z.2.2$ – ОКС «Частичный секретный ключ схемы открытого шифрования участника ЭДО»; $A.2.3$, ..., $Z.2.3$ – ОКС «Полный секретный ключ и открытый ключ схемы открытого шифрования участника ЭДО»; $A.3.1$, ..., $Z.3.1$ – ОКС «Идентификатор и персональный секретный ключ ПРК участника ЭДО»; $A.3.2$, ..., $Z.3.2$ – ОКС «Частичный секретный ключ ПРК участника ЭДО»; $A.3.3$, ..., $Z.3.3$ – ОКС «Полный секретный ключ и открытый ключ ПРК участника ЭДО»; K_{IJ} – ОКС «Общий секретный ключ участников I и J».

Примечание: Для повышения безопасности возможно применение следующих СУКМ: (x) – пороговых СРС или СРС, функционирующих в модели «проактивной безопасности»; (@) – схем эволюции ключей с изоляцией ключа; (+) – схем удаленного управления ключом.

5. Пример: расчет показателей безопасности КС однодоменной системы электронного документооборота с ИОК

По той же методике [3] проводится расчет показателей безопасности КС любых из описанных систем ЭДО. Рассмотрим пример такого расчета для системы защищенного ЭДО на основе ИОК.

Возьмем систему ЭДО без привязки к каким-либо конкретным программным средствам, но со структурой, соответствующей рисунку 1. Пусть она включает следующие объекты ключевой системы: УЦ «T_0», 3 системных сервиса ДТС («T_1», «T_2», «T_3») и не определенное заранее количество клиентов, каждый из которых имеет пары ключей для схемы цифровой подписи, схемы открытого шифрования и открытого распределения ключей.

УЦ реализован на технических средствах, обеспечивающих для каждого компонента ОКС коэффициент доступности $K_Д = 0{,}9999$, системные сервисы – $K_Д = 0{,}999$, клиенты – $K_Д = 0{,}995$.

Для расчета каждый ОКС в составе КС необходимо представить в виде графа. Для простоты будем предполагать, что ОКС «T_0», «T_1», «T_2», «T_3», «$X.1$», «$X.2$», где $\underline{X = A, Z}$, в основе своей имеют пару ключей, связанных функцией RSA. ОКС «X.3», где $X = A, Z$, в основе своей имеют пару ключей для протокола открытого распределения ключей Диффи–Хеллмана. На все открытые ключи системных сервисов и клиентов выдан сертификат УЦ. УЦ имеет самоподписанный сертификат. Параметры криптосистемы таковы: длина модуля для всех ключей – 1024 бит, длина сертификатов открытых ключей – 4 кбит, компоненты ОКС «9», «10», «11» – по 512 бит. Для контроля целостности применяется побайтная проверка на четность, т. е. длина проверочных разрядов равна 1/8 длины компонентов ОКС. Для всех компонентов ОКС и отдельных ОКС, содержащих параметры криптосистемы, показатели доступности, аутентичности и секретности принимаются нулевыми. Компрометация секретных ключей УЦ по экспертной оценке может происходить в среднем 1 раз в 10 лет, ключей ДТС – 1 раз в 5 лет, клиентских ключей – 1 раз в 3 года.

Требуется обеспечить следующие интегральные показатели безопасности (ИПБ) [10] элементов КС со структурой, показанной на рисунке 2, на временном интервале λ продолжительностью 1 месяц: для подсистемы SKS_1, состоящей из ключей УЦ и системных сервисов, – не ниже 0,95; для любой подсистемы SKS_2, состоящей из всех ключей одного клиента системы ЭДО, – не ниже 0,80; для любой подсистемы SKS_3, состоящей из всех ключей фиксированной пары клиентов и их общего секретного ключа, – не ниже 0,63.

При перечисленных условиях расчет дает показатели безопасности, показанные в таблице 1.

Таблица 1. Показатели безопасности КС однодоменной системы ЭДО с ИОК

Элементы КС / Показатели безопасности	ОКС				Подсистемы КС		
	«T_0»	«T_i», где $i = 1,2,3$	«$X.1$», «$X.2$», «$X.3$», где $X = A, ..., Z$	«K_{IJ}»	SKS_1	SKS_2	SKS_3
α	$6{,}00 \cdot 10^{-4}$	$5{,}99 \cdot 10^{-3}$	$2{,}96 \cdot 10^{-2}$	$9{,}98 \cdot 10^{-3}$	$1{,}85 \cdot 10^{-2}$	$8{,}62 \cdot 10^{-2}$	0,173
β	$8{,}33 \cdot 10^{-3}$	$8{,}33 \cdot 10^{-3}$	$8{,}33 \cdot 10^{-3}$	2^{-32}	$3{,}29 \cdot 10^{-2}$	$2{,}48 \cdot 10^{-2}$	$4{,}90 \cdot 10^{-2}$
γ	$8{,}33 \cdot 10^{-3}$	$1{,}67 \cdot 10^{-2}$	$2{,}78 \cdot 10^{-2}$	$5{,}55 \cdot 10^{-2}$	$5{,}72 \cdot 10^{-2}$	$8{,}11 \cdot 10^{-2}$	0,2025
S	0,983	0,969	0,936	0,935	0,895	0,819	0,627

Обозначения: «T_0» – ОКС «Ключи УЦ»; «T_1», «T_2», «T_3» – ОКС «Ключи ДТС»; «$X.1$» – ОКС «Ключи клиента для схемы ЭЦП»; «$X.2$» – ОКС «Ключи клиента для схемы открытого шифрования»; «$X.3$» – ОКС «Ключи клиента для ПРК»; «K_{IJ}» – ОКС «Общий секретный ключ клиентов I и J».

Полученные значения ИПБ для подсистем SKS_1 и SKS_3 не удовлетворяют предъявленным к системе требованиям. Для повышения показателей безопасности подсистем применим СУКМ к составляющим их ОКС: к ОКС «T_0» – (5,7)-пороговую СРС, к ОКС «T_1», «T_2», «T_3» – (3,5)-пороговую СРС, к ОКС «K_{IJ}» – схему дистанционного управления ключами (введем зависимость общего секретного ключа от разовых ключей протокола распределения ключей).

При этих условиях выполним пересчет частных и интегральных показателей безопасности. Результаты показаны в таблице 2.

Таким образом, ИПБ подсистемы SKS_1 повысился с 0,875 до 0,951, а ИПБ подсистемы SKS_3 – с 0,627 до 0,634. Требования к системе выполнены.

Таблица 2. Показатели безопасности КС однодоменной системы ЭДО с ИОК при условии применения СУКМ к некоторым ОКС

Элементы КС / Показатели безопасности	ОКС				Подсистемы КС		
	«T_0»	«T_i», где $i = 1,2,3$	«$X.1$», «$X.2$», «$X.3$», где $X = A, ..., Z$	«K_{IJ}»	SKS_1	SKS_2	SKS_3
α	$5{,}00 \cdot 10^{-4}$	$4{,}99 \cdot 10^{-3}$	$2{,}96 \cdot 10^{-2}$	$9{,}98 \cdot 10^{-3}$	$1{,}54 \cdot 10^{-2}$	$8{,}62 \cdot 10^{-2}$	0,165
β	$8{,}33 \cdot 10^{-3}$	$8{,}33 \cdot 10^{-3}$	$8{,}33 \cdot 10^{-3}$	$3{,}45 \cdot 10^{-77} \approx 0$	$3{,}29 \cdot 10^{-2}$	$2{,}48 \cdot 10^{-2}$	$4{,}90 \cdot 10^{-2}$
γ	$8{,}31 \cdot 10^{-10}$	$2{,}06 \cdot 10^{-4}$	$2{,}78 \cdot 10^{-2}$	$5{,}48 \cdot 10^{-2}$	$6{,}18 \cdot 10^{-4}$	$8{,}11 \cdot 10^{-2}$	0,2019
S	0,991	0,987	0,936	0,945	0,952	0,819	0,634

Обозначения: «T_0» – ОКС «Ключи УЦ»; «T_1», «T_2», «T_3» – ОКС «Ключи ДТС»; «$X.1$» – ОКС «Ключи клиента для схемы ЭЦП»; «$X.2$» – ОКС «Ключи клиента для схемы открытого шифрования»; «$X.3$» – ОКС «Ключи клиента для ПРК»; «K_{IJ}» – ОКС «Общий секретный ключ клиентов I и J».

Заключение

В работе осуществлен синтез ключевых систем средств организации защищенного электронного документооборота, построенных на основе инфраструктуры открытых ключей, идентификационных и бессертификатных криптосистем. С помощью разработанной автором методики структурно-параметрического синтеза ключевых систем СКЗИ проведены расчеты показателей безопасности модельной системы защищенного электронного документооборота на основе инфраструктуры открытых ключей, продемонстрированы возможности повышения показателей ее безопасности путем применения схем управления ключевым материалом.

СПИСОК ЛИТЕРАТУРЫ:

1. *Запечников С. В.* Криптографические особенности применения функций шифрования и цифровой подписи в электронном документообороте и в электронной коммерции // Безопасность информационных технологий. 2005. № 2. С. 55–63.
2. *Запечников С. В.* Модельное представление ключевых систем средств криптографической защиты информации // Безопасность информационных технологий. 2008. № 4. С. 84–92.
3. *Запечников С. В.* Синтез ключевых систем средств криптографической защиты информации и определение показателей их стойкости в условиях воздействия дестабилизирующих факторов // Научная сессия МИФИ-2009. Сборник научных трудов. Часть 1: Научные достижения университета. М.: МИФИ, 2009.
4. *Запечников С. В.* Повышение стойкости средств криптографической защиты информации на основе применения схем управления ключевым материалом // Материалы XII Международной конференции «Комплексная защита информации», Ярославль, 2008 г. М.: РФК-Имидж Лаб, 2008. С. 85–87.
5. *Shamir A.* Identity-based cryptosystems and signature schemes // Adv. in Cryptology – Proc. of CRYPTO'84, LNCS, Vol. 196. Springer-Verlag, 1985. P. 47–53.
6. *Boneh D.* Identity-Based Encryption from the Weil pairing // Adv. in Cryptology – Proc. of CRYPTO'2001, LNCS, Vol. 2139. Springer-Verlag, 2001. P. 213–229.
7. *Boneh D.* Short Signatures from the Weil Pairings // Adv. in Cryptology – Proc. of ASIACRYPT'2001, LNCS, Vol. 2248. Springer-Verlag, 2001. P. 514–532.
8. *Al-Riyami S.* Certificateless public key cryptography // Adv. in Cryptology – Proc. of Asiacrypt'2003, LNCS, Vol. 2894. Springer-Verlag, 2003. P. 452–473.
9. *Liu J. K.* Self-Generated-Certificate Public Key Cryptography and Certificateless Signature/Encryption Scheme in the Standard Model [электронный ресурс]. URL: http://eprint.iacr.org/2006/373.
10. *Запечников С. В.* Принципы обеспечения стойкости криптосистем к компрометации ключей // Безопасность информационных технологий. 2008. № 1. С. 80–86.