**ВАЛЕРИЙ АНДРЕЕВ,**
заместитель директора по науке и развитию компании ИВК, к.ф.-м.н.

# Особенности обработки документов ограниченного доступа в СЭД с различным уровнем конфиденциальности на территориально распределенной информационной инфраструктуре

Актуальной задачей систем электронного документооборота (СЭД) на современном этапе развития ИТ-отрасли остается задача объединения, интеграции в единый процесс обработки электронных документов разрозненных удаленных информационных объектов заказчика, должностных лиц (ДЛ) на этих объектах, для обеспечения управляемости сквозным (возможно, даже оперативным) обменом документами, часто – ограниченного доступа с различным уровнем конфиденциальности. Важным моментом в такого рода обмене является обеспечение гарантии информационного взаимодействия на комплексе разрозненных объектов автоматизации, связанных к тому же разнородными, недоверенными каналами связи, особенно в случае реализации технических решений для юридически значимых СЭД. Таким образом, для многих заказчиков суть очередного витка информатизации в СЭД состоит в обеспечении оперативного юридически значимого обмена документами (в том числе ограниченного доступа) на основе предписанной логики взаимодействия должностных лиц заказчика, объектов его инфраструктуры, процессов в них.

Полноценное внедрение электронной подписи (ЭП) в таких СЭД, по-видимому, не сможет изменить существующее положение дел и «подтянуть» актуальные СЭД на новый уровень, поскольку не допускает применения к таким документам и ограничивается уровнем «конфиденциально». Утилизация всех возможностей технологии PKI (Public Key Infrastructure – инфраструктура открытых ключей) на всем жизненном цикле электронного документа: от создания, согласования, ознакомления, утверждения к рассылке, контролю исполнения, защите и пр. остается весьма актуальной, но может рассматриваться в указанных системах лишь в качестве дополнительного средства повышения доверия.


SHUTTERSTOCK.COM/THREECVET.GMAIL.COM

Внедрение технологии PKI (КриптоПро, СКБ «Контур», СигналКом и пр.) на прикладной уровень также остается известной проблемой для организации SSO (Single-Sign-On – однократная авторизация пользователя на информационных ресурсах). Зачастую рабочее место должностного лица буквально «утыкано» разными USB-устройствами хранения ключевой информации, относящимися к разным приложениям. То же можно отнести к предлагаемым разным ключевым парам для обработки информации различной степени конфиденциальности у одного физического лица. Все эти особенности приводят к общей хаотизации процедуры предъявления идентификационной и аутентификационной информации и находятся столь далеко от желаемого SSO, что оно уже начинает казаться утопией.

На этом проблематика защиты СЭД отнюдь не заканчивается. Насущной необходимостью современного этапа развития СЭД является учет важнейшего свойства электронных (и бумажных) документов – расщепления по принципу конфиденциальности отражаемой в документе информации. Действительно, в реальных информационных системах не существует «плоского» потока однородной информации. Любой документ имеет собственную метку конфиденциальности, так называемый «гриф», позволяющий отразить степень его конфиденциальности и, таким образом, заранее предусмотреть необходимые механизмы и меры по обеспечению его жизненного цикла. Документы с разными «грифами» обрабатываются, хранятся, передаются и контролируются по-разному в разных операционных средах (ОС, СУБД, СЗИ и пр.). Поэтому указанное многообразие средств аутентификации пользователя в реальных системах умножается где-то на два, чаще на три, и на столах должностных лиц устанавливаются по нескольку компьютеров из сетей разной степени «секретности», что жизнь их также не упрощает. Применение различных СЭД в различных контурах безопасности настолько усложняет работку ДЛ и решение задачи защиты информации, что сегодня представляется нереалистичным (например, в части «наследования грифа» документа).

Многое в этих процессах зависит от самих должностных лиц, в особенности от руководителей высшего звена, которые зачастую просто выпадают из общих процессов СЭД, оставаясь в них лишь физическими лицами, доверяя свои функции назначенным ими доверенным лицам. Вопросы, связанные с доверием к этим доверенным лицам, в СЭД также находятся в зачаточном состоянии.

## Основные требования к актуальным системам защищенного документооборота

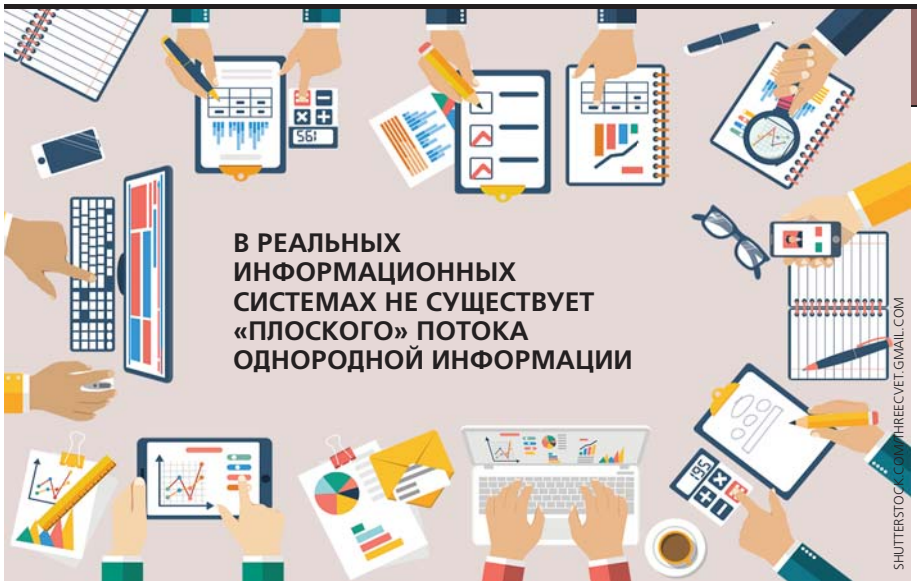
Исходя из вышеуказанных предпосылок можно в общих чертах сформулировать некоторые требования к актуальным системам защищенного юридически значимого электронного документооборота, которые так или иначе придется выполнять в обозримом будущем всем производителям СЭД:

- Функционирование СЭД на разнородных программно-аппаратных платформах.
- Создание территориально распределенных решений для СЭД, учитывающих специфику функционирования на территории РФ.
- Обеспечение гарантированной доставки подписанных электронных документов в режимах коллективной или избирательной обработки, «с контролем исполнения» и пр.
- Поддержка серверов каталогов (AD, LDAP, ALD или иное) для глобальной идентификации ДЛ на реальной инфраструктуре объектов СЭД.
- Использование ЭП во всем жизненном цикле электронного документа для создания полноценной юридически значимой СЭД, в том числе с использованием внешних соединений с Удостоверяющим центром(ами) (УЦ). Сегодня может рассматриваться лишь как дополнительное средство повышения доверия к отправлению в связи с ограничением в применении на уровне «конфиденциально».
- Единообразное функционирование в различных контурах (средах) обработки документов (в том числе ограниченного доступа) с обеспечением безопасного взаимодействия средств СЭД в контурах безопасности.
- Обеспечение глобального поиска документов с учетом единой политики информационной безопасности.
- Дополнительное введение в СЭД службы единого времени для создания систем электронного нотариата (при необходимости).

В результате должна быть решена сверхзадача – автоматизация рутинных процессов обработки электронных документов различного уровня конфиденциальности в соответствии с логикой обработки заказчика на распределенной информационной инфраструктуре в системах с юридически значимым документооборотом.

Реализация указанных требований требует принципиального изменения отношения СЭД к средствам передачи и хранения данных – встроенных или внешних, – так как для указанной реализации необходимы такие средства, которые обеспечивали бы гарантированные сервисы информационного взаимодействия и хранения документов не только при условии произвольных каналов связи и произвольной топологии связанных объектов автоматизации, но и наличия на этих объектах различных контуров обработки документов. Важнейшим аспектом современного функционирования СЭД является наличие фактора динамического (мобильного) подключения авторизованных пользователей (должностных лиц) к ее информационным ресурсам, распределено хранящимся в информационных системах объектов автоматизации заказчика.

В связи с этими требованиями возможно создание сложного централизованного решения, контурирование в котором будет осуществляться на уровне средств хранения, а контроль доступа – на уровне средств разграничения доступа также из состава подсистемы хранения и отчасти – сервера приложений. Одна-




ко же эта задача сегодня не решена, по-видимому, в связи с отсутствием таковых. Можно отнести ее к задачам будущего.

Здесь же возникает вполне разумная концепция применения в архитектуре СЭД такого элемента, как универсальная защищенная интеграционная шина. Возможности ее в достаточной степени изучены и реализуются посредством следующих важнейших принципов:

- предоставление типовых гарантированных сервисов по обмену данными и оперативному управлению объектами и процессами в СЭД;
- обеспечение гарантированного взаимодействия прикладных подсистем на объектах СЭД на основе асинхронной (синхронной) модели обмена данными;
- предоставление сервиса гарантированного хранения собственных данных ДЛ и ключевой информации, необходимой для функционирования прикладных процессов;
- обеспечение управляемости единым вычислительным процессом на объектах СЭД на основе общесистемных соглашений;
- обеспечение защиты информации в СЭД на основе единой непротиворечивой политики безопасности;
- единообразное функционирование СЭД в различных программно-аппаратных средах исполнения, формируемых ОС, СУБД, СЗИ и иными средствами;
- наличие стандартных интерфейсов и инструментария прикладного программирования для решения задач интеграции данных.

Реализация актуальных требований к СЭД становится вполне возможной на такой платформе. Одним из основных вопросов функционирования СЭД на распределенной инфраструктуре становится, таким образом, упорядочение процедур обмена документами (в том числе ограниченного доступа) с максимальной автоматизацией последних, а также вполне вероятное подключение СЭД к унаследованным системам обмена, а также существующим «входящим потокам» документов типа МЭДО, СМЭВ и прочее. Использование такой платформы позволит отказаться от централизации системы обработки документов в пользу распределения по объектам, что даст возможность объектам СЭД работать самостоятельно в случае отсутствия связи с центром.

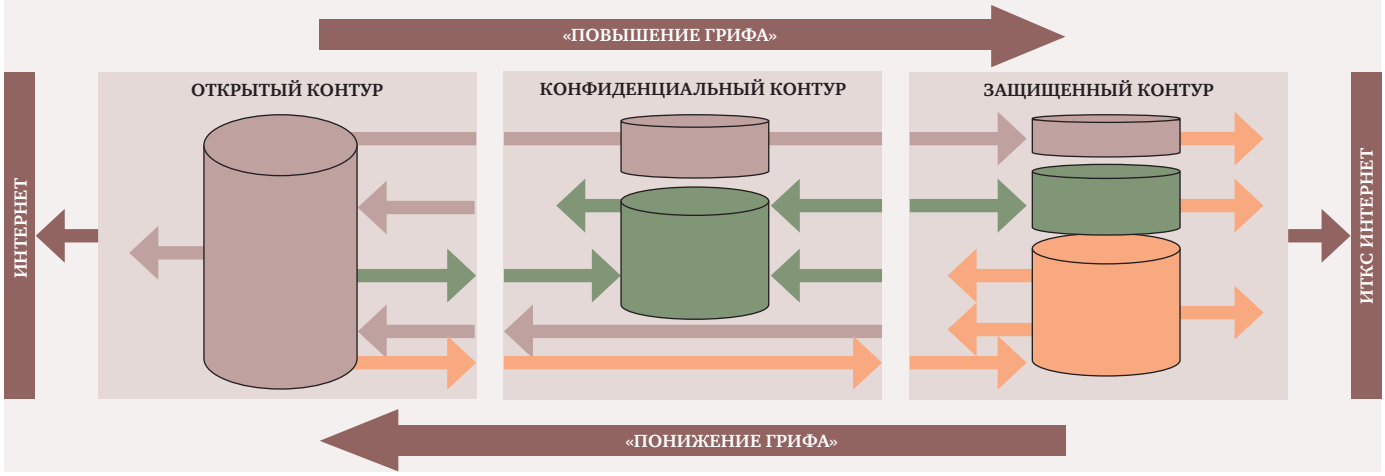
## Обработка данных различных уровней конфиденциальности (контурирование)

Сегодня существует необходимость напоминания о принципиальных моментах в обработке документов с «грифом». Для многих реальных задач защищенного электронного документооборота и ряда конкретных заказчиков существует необходимость обеспечения контурирования объектов автоматизации по принципу расщепления грифа и, как следствие, создания контуров безопасности, обеспечивающих обработку документов с разными метками конфиденциальности. Заметим, что контуров безопасности может быть несколько – столько, сколько типов различной по степени конфиденциальности информации циркулирует в системах заказчика и определяется им в основополагающих документах по ИБ. Предположим, что таких контуров три: открытый, конфиденциальный и защищенный, и, следовательно, грифа будет тоже три – «о», «к» и «з». Особую актуальность сегодня имеет задача обеспечения циркуляции различных типов информации между контурами безопасности, например:

- Открытая информация может свободно циркулировать между всеми контурами преимущественно в одну сторону – в сторону «повышения грифа». Обратное взаимодействие возможно только при выполнении необходимых механизмов и процедур «понижения грифа». Межъобъектовый обмен информацией осуществляется посредством сети Интернет (через межсетевой экран – МЭ) только из открытого контура – единственного из контуров, имеющего такое прямое соединение.
- Информация ограниченного распространения конфиденциального контура может циркулировать между конфиденциальным и защищенным контурами также преимущественно в сторону «повышения грифа». Обратное взаимодействие возможно только при «понижении грифа». Обмен информацией осуществляется посредством наложенной защищенной сети, функционирующей «поверх» Интернет, реализуемой обычно посредством сертифицированных криптосредств (шифратор, маршрутизатор и пр.) необходимого уровня конфиденциальности.
- Информация ограниченного доступа защищенного контура может циркулировать только внутри и между защищенными контурами. Взаимодействие с прочими контурами возможно только при «понижении грифа». Обмен информацией часто осуществляется посредством создания выделенной защищенной информационно-телекоммуникационной системы (ИТКС) по специализированным каналам связи, а также и при помощи сертифицированных криптосредств более высокого уровня.

Логическая схема разграничения контуров в случае «вертикального» обмена выглядит на рисунке 1.

Рисунок 1. Циркуляция информации различного уровня конфиденциальности




Зеленым цветом показан открытый контур безопасности объекта автоматизации, синим – конфиденциальный контур безопасности, красным – защищенный контур. Стрелками показаны «восходящие» потоки информации (зеленый – открытая информация, синий – информация ограниченного распространения, красным – информация ограниченного доступа). На каждом «пересечении» границы контура необходимо выполнение процедуры «понижения грифа» – шифрования, фильтрации, маршрутизации, наследования грифа и пр. Межобъектовый обмен в рамках информационной инфраструктуры заказчика должен обеспечиваться такими средствами, которые имели бы встроенные возможности по передаче указанной, уже «расщепленной» информации в едином канале связи для снижения общих расходов по поддержанию функционирования самой СЭД.

В любом случае необходимо помнить, что «гриф» устанавливает должностное лицо, причем на основе определенных внутренних документов, обеспечивающих невозможность как «занижения», так и «завышения» грифа ответственным исполнителем. За этим приходится пристально следить. Кроме того, «входящий гриф» должен наследоваться, т. е. адекватно отображаться, обрабатываться и передаваться средствами актуальной СЭД, даже если внешний поток документов реализуется на иных программных средствах третьей стороны.

Создание актуальных СЭД с такой логикой обработки плюс определение самого понятия «электронный документ» и организация его обработки с меткой конфиденциальности – важная задача СЭД! Особое внимание в этом случае уделяется ЭП, поскольку предполагается, что в разных контурах безопасности «работает» своя ЭП. Однако эта сложная в реализации предпосылка на сегодняшний день не актуальна. Поэтому обработка ЭП в защищенном контуре является необязательной, ЭП в нем можно рассматривать лишь как дополнительное средство защиты, и то при условии, что они обрабатывается в операционной среде защищенного контура.

Дополнительно можно отметить, что в Федеральном законе № 63-ФЗ «Об электронной подписи» от 06.04.2011 г. нет ни слова о метках конфиденциальности (грифах), а в Федеральном законе № 5485-1 «О государственной тайне» от 08.03.2015 г. не ни слова об электронной подписи. В связи с этим разрывом и обработка документов в юридически значимых СЭД ведется ограниченно, в соответствии с пониманием заказчика и исполнителя, начиная от определения самого понятия – «электронный документ ограниченного доступа».

## Возможности актуальных СЭД

Наличие указанного «разрыва» и общей незаполненности нормативно-правовой базы в случае обработки электронных документов (в ом числе ограниченного доступа) неизбежно приводит к почти автоматической трансляции правил обработки «бумажных» документов в качестве правил обработки электронных документов. Причем правила эти являются ведомственными и существенно меняются от заказчика к заказчику. Во многих случаях особенности обработки таких документов просто не поддаются нормальной реализации. В некоторых случаях приводят к существенной переработке уже готовых продуктов (с их последующей сертификацией по требованиям регуляторов). Одним из примеров может быть весьма распространенное понятие «копийность», которое означает рассылку электронного документа с признаком «Экз.№___», т. е. номер копии документа, который еще к тому же ассоциируется с порядком исполнителей в списке рассылки. Иногда заказчик требует автоматической печати этого атрибута на титульной станице документа. Как, впрочем, и вообще контроля средств печати средствами СЭД, что уже вовсе из разряда фантастики. Словом, как обычно, «за неимением гербовой – пишем на простой». Чем быстрее отрасль разберется с таким «наследием» привычной «бумажной» обработки, тем быстрее у нас появятся такие СЭД, которые позволят должностным лицам работать на ОДНОМ компьютере, с ОДНОЙ ЭП, на ОДНОМ (своем) рабочем месте, в ОДНОМ приложении, но безопасно решать при этом МНОГО задач – оперативно, разумно и недорого.

Все это уже сегодня возможно при помощи отечественных сертифицированных продуктов, сориентированных для использования в разнородных территориально распределенных системах юридически значимого оборота электронных документов (в том числе ограниченного доступа). ●