Защищенный документооборот на платформе Sun-Documentum

Р. М. Рыжков
Технологическая лаборатория ОАО «Элвис+»

О системах электронного документооборота написано много и многими. Кажется, все уже сказано на тему их актуальности, преимуществ и удобства для пользователей. И пожалуй, не впустую сказано. Примеры в той или иной степени успешного внедрения СЭДО на базе продуктов различных компаний, как отечественных, так и зарубежных, известны. Слова «в той или иной степени успешного» здесь использованы не как выпад, скорее это попытка отметить объективные трудности внедрения. Как правило, установленные и настроенные системы электронного документооборота вполне работоспособны. А вот их активное практическое применение сдерживается различными факторами. Не на последнем месте среди них стоят и проблемы, связанные с обеспечением необходимого уровня безопасности информации в системе.

В традиционных, бумажных, системах документооборота используется комплекс мер, обеспечивающих доверие к содержанию документов. Это регламент регистрации документов, подписи, печати и т. д. Такие мероприятия обеспечивают сохранность документов и регламентированный доступ к ним. Для того чтобы электронный документ мог использоваться вместо бумажного, необходимо также обеспечить доверие пользователя к его содержанию, предотвратить несанкционированные изменения и возможность утери (разрушения), организовать регламентированный доступ пользователей к документам. Это вполне соответствует классическим целям защиты информации – обеспечению ее доступности, целостности и конфиденциальности.

Формулировка «защищенный документооборот» применялась и применяется к системам, решающим хотя бы часть задач информационной безопасности. Использование в электронном документообороте технологий виртуальных частных сетей (VPN), или применение электронно-цифровой подписи, или шифрование хранимых данных давало повод назвать его защищенным. Однако систем, обеспечивающих безопасность информации по всем направлениям, к тому же отвечающих требованиям отечественных нормативных документов, пока не много.

Одна из них – система электронного документооборота, функционально ориентированная на планирование и сопровождение НИОКР. Решение обеспечивает полноценную коллективную работу с электронными документами с учетом территориально распределенной организационной структуры заказчика, интеграцию с традиционно при-

меняемыми автоматизированными системами, безопасность обрабатываемой и хранимой информации.

Требования к обеспечению безопасности информации

Система электронного документооборота создавалась для использования в двухуровневой структуре, включающей Центральный узел и узлы регионального уровня. Например, система может включать Федеральный центр планирования и сопровождения НИОКР и подчиненные ему узлы в субъектах Российской Федерации. Может быть реализована и трехуровневая схема (Центр – Федеральные округа – субъекты РФ). Сегменты разных уровней аналогичны по структуре и выполняемым функциям, но могут различаться по составу и моделям технических средств, в зависимости от предполагаемой нагрузки.

Внутри каждого сегмента решаются задачи защиты серверов, автоматизированных рабочих мест и рабочих станций от несанкционированного доступа, а также антивирусной защиты. Также безопасность информации обеспечивается путем организации регламентированного доступа и предотвращения несанкционированного доступа к документам СЭДО и прочей информации системы.

Территориально распределенная структура делает актуальными задачи репликации и синхронизации данных между узлами различных уровней как в условиях устойчивой связи между ними, так и в режиме сеансовой связи. С этой точки зрения важны возможности по защите периметра территориальных сегментов СЭДО от несанкционированного доступа и организации защищенных каналов связи между сегментами.

Решение поставленных задач достигается наряду с распространенными и хорошо зарекомендовавшими себя методами также с помощью гораздо реже используемых средств.

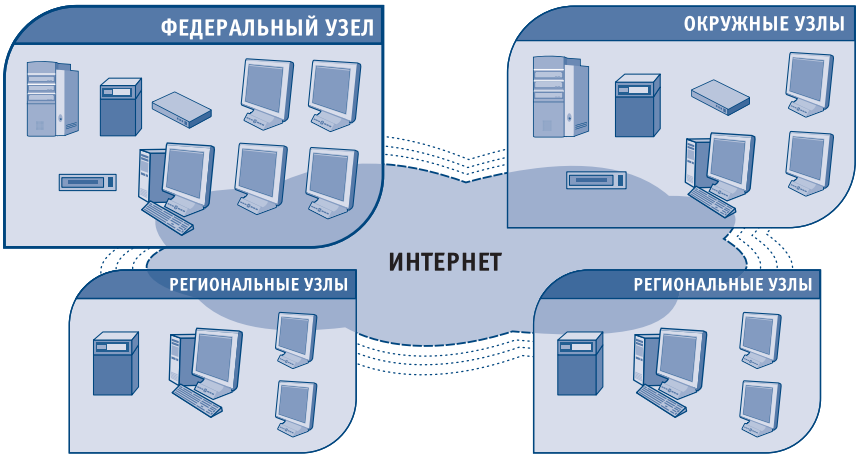

Рис. 1. ***Территориально распределенная система документооборота***

При создании системы учитывались требования по ее соответствию отечественным нормативным документам в области информационной безопасности.

Описание системы. Sun, Solaris и терминалы

Средства и методы обеспечения информационной безопасности коренным образом зависят от того, какие технические и программные средства используются в качестве базовых при построении системы, какова ее общая структура. Как упоминалось, описываемый вариант представляет собой двух-, трехуровневую территориально распределенную систему. Сегменты разных уровней имеют аналогичную структуру и функциональность. Для их построения применяются технические средства из одной линейки, отличающиеся производительностью.

Поскольку задачи обеспечения информационной безопасности были обозначены как приоритетные при создании системы, к подбору техники и базового ПО было проявлено особое внимание.

Для создания технической платформы системы были выбраны серверы компании Sun Mycrosystems. Систему решено было строить на основе терминальных технологий той же компании Sun. Таким образом, основная часть аппаратного комплекса решения включала RISC – сервер линейки Sun Fire (использовались модели от простейшей V280 до высокопроизводительной V880) и комплект терминалов Sun Ray170 thin client.

Сервер работает под управлением операционной системы Trusted Solaris 8, а в качестве основы прикладной системы на сервере установлено ПО Documentum, принадлежащее одному из мировых лидеров в производстве программного обеспечения для электронного документооборота.

Кроме создаваемой системы электронного документооборота любой заказчик, конечно же, уже использует ряд привычных приложений, таких как MS Office, Exchange, бухгалтерские системы и т. д. Речь идет о приложениях, работающих на Windows/Intel платформе.

Как зачастую решается вопрос о внедрении у такого заказчика новой информационной системы, использующей технику и терминальные технологии Sun Microsystems? Наверное, многим доводилось видеть, что решение бывает самым простым: рядом с Windows-сервером на платформе Intel устанавливается RISC-сервер Sun, а на рабочем столе пользователя рядом с персональным компьютером появляется терминал SunRay. Недостатки такого решения очевидны, и при создании системы документооборота был избран другой подход.

Получать доступ к любым системам, работающим на терминальном сервере Sun Fire, с терминалов Sun Ray 170 позволяет программное обеспечение SunRay Server Software 2.0. В свою очередь, клиент межплатформенного доступа Citrix обеспечивает связь терминального сервера Sun с сервером, на котором под управлением ОС MS Windows 2003 Server выполняются унаследованные

приложения, такие как традиционные MS Office, Exchange и др. Это позволяет работать с Windows-приложениями с тех же терминалов Sun Ray, с которых осуществляется доступ к UNIX-приложениям.

Такова в основном, программно-техническая конфигурация системы, особенности которой повлияли на методы обеспечения информационной безопасности. Для полноты описания упомянем, что в качестве основного средства работы с документами форматов *.doc и *.txt используется программное обеспечение Star Office 7 Upd 5 компании Sun Microsystems. Функционально пакет подобен Microsoft Office и имеет схожий графический интерфейс. Его принципиальным отличием является способность работать под управлением различных операционных систем, таких как различные версии Linux и UNIX, в том числе UNIX Trusted Solaris. Для выполнения приложений Documentum, таких как Webtop (обеспечивающий функционирование «тонкого» клиента) и Documentum Administrator (обеспечивающий функционал администрирования), используется сервер приложений Tomcat 5.0.2.8. В качестве программного «тонкого» клиента в системе используется интернет-браузер Mozilla 1.7.3.

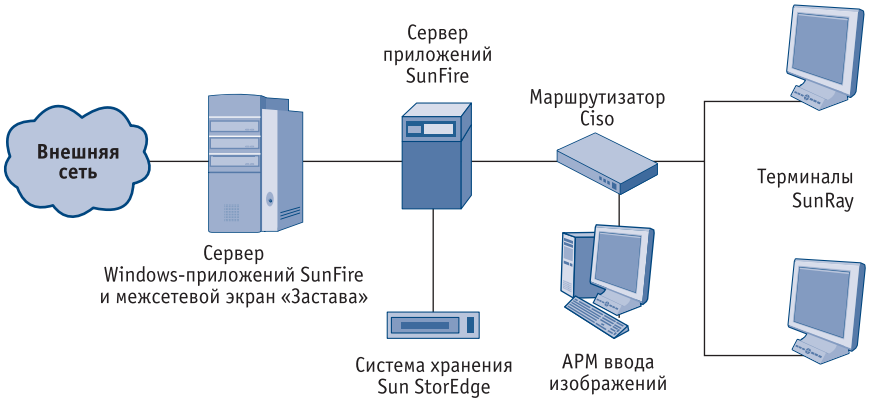

Рис. 2. ***Типовой узел системы***

Механизмы информационной безопасности

На первый взгляд, описанная программно-техническая архитектура решения вовсе не кажется очевидной. Но для начала давайте обратим внимание на такие ее особенности, как использование терминальных технологий и применение операционной системы Trusted Solaris.

В системе использована широко сегодня известная, но мало распространенная в нашей стране архитектура построения решения, основанная на использовании в качестве рабочих мест пользователя аппаратных «тонких клиентов», иначе называемых терминалами. Терминал представляет собой монитор с клавиатурой и мышью и лишен привычных атрибутов персонального компьютера: материнской платы и универсальных процессоров, жесткого диска и дискет, привода для компакт-дисков, портов для подключения принтера. Это устройство не предназначено для размещения и выполнения на нем программ, а служит лишь для доступа через локальную сеть к серверу, на котором происходит хранение и обработка информации, управление пользователями и реализуются прочие функции информационной системы. В решении использованы терминалы Sun Ray 170.

Чем хороши терминальные решения с точки зрения защиты информации? Они лишают пользователя многих возможностей, порождающих угрозы информационной безопасности, или просто не предусмотренных функциональными обязанностями сотрудника. Так, работая за терминалом, нельзя скопировать на дискету или флэш-карту информацию, нельзя установить на рабочее место вредоносное или просто не разрешенное к использованию программное обеспечение. Доступ к такому терминалу пользователь может получить, введя имя пользователя и пароль или вставив в считыватель, имеющийся в терминале, пластиковую карту с персональной идентификационной информацией. В описываемом решении доступ по имени и паролю запрещен, и получить доступ к системе может только обладатель смарт-карты. Таким образом, решается часть задачи предотвращения несанкционированного доступа к системе.

Итак, пользователь предъявил терминалу свою карту-идентификатор, система произвела аутентификацию и определила, какими правами доступа к тем или иным объектам системы UNIX наделен пользователь. К сожалению, известны случаи, когда даже в такой надежной операционной системе, как UNIX Sun Solaris, искушенный (и злонамеренный!) пользователь может получить доступ к закрытой для него информации. Для предотвращения такого рода инцидентов была разработана версия ОС под названием Trusted Solaris 8. Она реализует такие усиленные механизмы защиты информации, как мандатный доступ и метки безопасности. Реализация этих возможностей в рамках операционной системы позволяет решить множество проблем с приложениями.

Имеются и другие средства информационной безопасности в рамках ОС Trusted Solaris. Например, каждому пользователю можно разрешить доступ к ограниченному числу привилегированных ресурсов, действительно ему необходимых. Имеются средства управления правами отдельных процессов (Process Rights Management) и расширенная технология управления правами пользователей (User Rights Management). Имеется защищенная графическая оболочка, не позволяющая одним программам получать контроль над окнами других программ. Trusted Solaris обеспечивает контроль доступа к периферийным устройствам, например, существует возможность организации обязательного сравнения метки документа, отправляемого на печать, с меткой принтера, позволяющего гарантировать, что конфиденциаль-

ные документы будут распечатаны только на доверенных принтерах.

В прессе были уже сообщения, что компании Sun Microsystems и ЗАО «МВП Свемел» завершили сертификацию аппаратно-программного комплекса, состоящего из разновидности операционной системы Solaris и терминалов Sun Ray. Целью проекта было создание среды, удовлетворяющей требованиям по безопасности, предъявленным российскими нормативами. Для этого корпорация Sun Microsystems предоставила партнеру исходные тексты операционной системы Solaris. Российские разработчики добавили в ОС возможность использования отечественных криптоалгоритмов. Именно эта операционная система с модифицированными возможностями шифрования и организации защищенных соединений и была положена в основу описываемой системы электронного документооборота.

Выше было рассказано о подходе к обеспечению безопасности информации, основанном на терминальных технологиях Sun и использовании защищенной операционной системы, к тому же соответствующих ряду отечественных требований к защите информации. Однако в системе используются и другие, более распространенные средства защиты.

В качестве средства, предотвращающего НСД к серверам и компьютерам системы, используются электронные замки «Криптон». Они обеспечивают разграничение и контроль доступа к серверам (компьютерам) и их аппаратным ресурсам, а также контроль целостности программной среды и имеют необходимые сертификаты. Антивирусная защита серверов обеспечивается продуктами McAfee.

Защита периметра сети, в которой располагается система документооборота, реализует межсетевой экран «Застава». Внутреннее сегментирование ЛВС осуществляется с помощью маршрутизаторов Cisco. Решить задачу единого управления политиками безопасности МЭ ЗАСТАВА и устройств Cisco удалось благодаря применению в системе программного комплекса «Застава-Управление».

Описанные средства позволяют как фактически обеспечить информационную безопасность документооборота, так и удовлетворить формальным требованиям, предъявляемым к защите конфиденциальной информации.

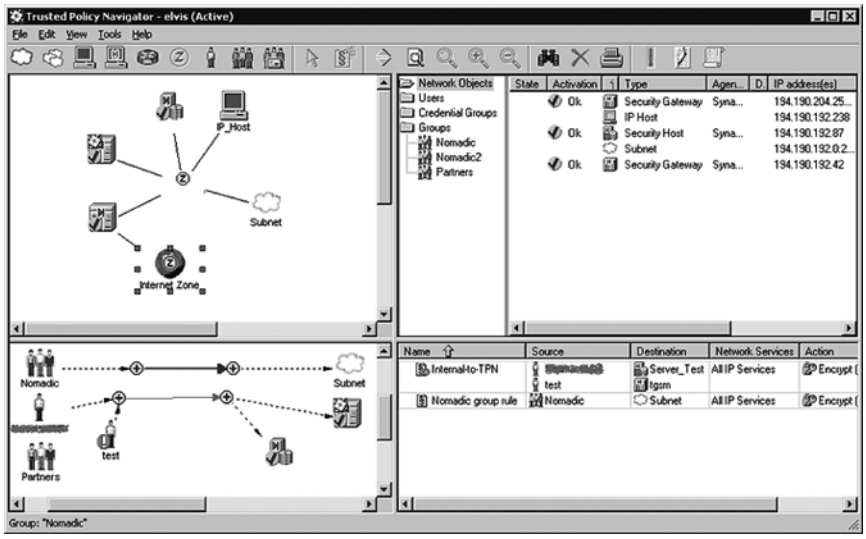

Рис. 3. ***Застава-Управление. Контроль информационной безопасности***

До сих пор вопросы информационной безопасности мы рассматривали, как бы не касаясь основы функциональной части – системы электронного документооборота Documentum. «Как бы» сказано не случайно. Documentum, являющийся ядром решения, оперирует двумя видами объектов для хранения информации. Первый – файлы, папки и каталоги операционной системы Sun Solaris, в которых и хранятся обрабатываемые документы. Второй – таблицы и записи базы данных Oracle, в которых хранится метаинформация, например карточка документа, сведения об его истории, маршруте его движения и т. д. Объекты операционной системы, как мы уже показали, надежно защищаются средствами Trusted Solaris. Защита же метаинформации осуществляется с использованием любых возможностей, встроенных в СУБД Oracle.

Заключение

Защита информации в территориально распределенной системе электронного документооборота, созданной на основе программных продуктов Documentum, обеспечивается несколькими путями.

Первый – применение терминальных технологий Sun Microsystems и защищенной операционной системы Sun Trusted Solaris с интегрированными в нее средствами российской криптографии. Второй – использование в системе сертифицированных замков «Криптон», сертифицированных средств защиты периметра семейства «Застава» и антивирусных средств.

В системе решена задача обеспечения доступа как к ее базовой части, работающей под управлением Trusted Solaris 8, так и к унаследованным приложениям, работающим под ОС семейства Windows, с терминала Sun Ray.

Построение системы на основе типовых сегментов позволяет легко масштабировать ее, увеличивая количество сегментов и включая в них технические средства соответствующей производительности. В сегментах использованы одинаковые схема и технология построения системы информационной безопасности.

Деятельность компаний, поставляющих базовое программное обеспечение и технику, и компаний, занимающихся защитой информации, позволяет надеяться, что в недалеком будущем системы электронного документооборота на базе продуктов Documentum, техники и технологий Sun Microsystems будут пригодны и для обработки информации, содержащей государственную тайну. ■