Защищенный документооборот DocsVision

Представление общей концепции защищенного документооборота (гарантии сохранения конфиденциальности информации, ее достоверности и обеспечения надежного хранения) на примере системы DocsVision.

Введение

Все больше компаний из различных отраслей внедряют системы электронного документооборота. При этом важнейшую роль для ведения бизнеса играют гарантии сохранения конфиденциальности информации, ее достоверности и надежного хранения.

В рамках данной статьи, на примере возможностей системы DocsVision, мы поговорим об общей концепции и понимании того, что такое защищенный документооборот и какими способами его можно защитить.

Разграничение прав в системе DocsVision

Система DocsVision – одна из первых систем, получивших сертификат о защите персональных данных по ФЗ 152, – может использоваться в составе ИСПДн до класса К2 включительно. На многих предприятиях система электронного документооборота используется не только как инструмент, обеспечивающий хранение документов, работу с ними, но и как система, позволяющая ограничить доступ пользователей к информации, что позволяет сотрудникам организации работать только с теми документами, с которыми они обязаны работать, и не использовать чужие, не нужные в работе документы. Сотрудники лишаются соблазна просматривать не касающуюся их информацию, и, тем более, копировать и изменять ее. При использовании защищенного документооборота, ограничивается круг лиц, принимающих участие в работе с данными, чтобы контролировать процесс работы с защищенным документом и знать, откуда возможна утечка информации. В системе DocsVision данный сценарий может быть реализован в рамках разграничения прав доступа, т.е на уровне дискретной безопасности с применением прав Active Directory. Вторым вариантом осуществления контроля работы с документами может быть мандатная безопасность, т.е. предоставление любому объекту системы, будь то папка, карточка документа и т.д., уровня доступа, наподобие грифов “секретно” или “совершенно секретно”. Таким образом, пользователи, имеющие уровень доступа “низкий”, не могут обратиться к папке и документам, имеющим уровень “средний” и выше.

Данный сценарий защиты может использоваться в случае, если имеется определенный круг лиц, например, руководителей департаментов, которые наделены одинаковыми правами доступа в рамках дискретной безопасности, но двое из них – это руководители департаментов, связанных с коммерцией, остальные лица – руководители производственных департаментов. Предположим, что производственному департаменту в работе не нужны данные коммерческого характера. Для того, чтобы ограничить доступ производственных руководителей к данной информации, на документы, относящиеся к коммерческой тайне, ставится гриф “уровень доступа выше среднего”, и точно такой же уровень дается руководителям коммерческого департамента. В данном случае не нарушаются общие права (дискретная безопасность) руководителей по работе с документами и папками, но одним простым действием, без применения матриц безопасности, ограничивается уровень доступа (рис. 1).

Помимо ограничения доступа средствами дискретной и мандатной безопасности, использующейся в системе DocsVision, можно обеспечить сотрудникам работу с документами как индивидуальную, так и коллективную, но в то же время исключается возможность утраты информации.

Совместная работа над документом позволяет сотрудникам постоянно отсле-

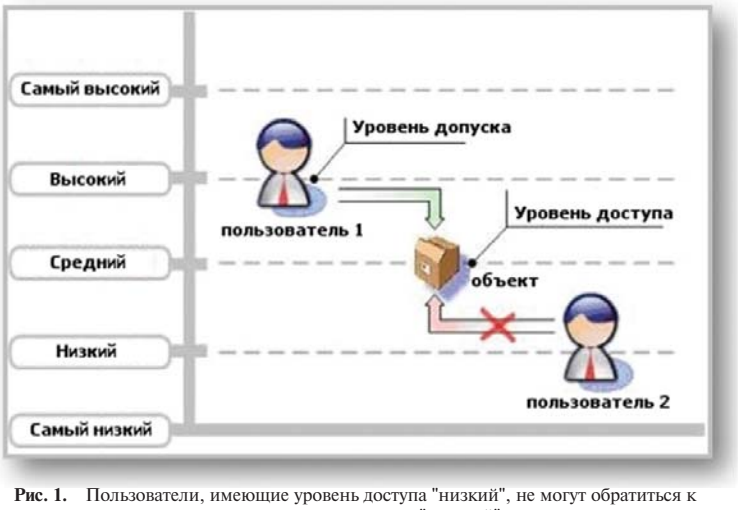

Рис. 1. Пользователи, имеющие уровень доступа "низкий", не могут обратиться к папке и документам, имеющим уровень "средний" и выше.

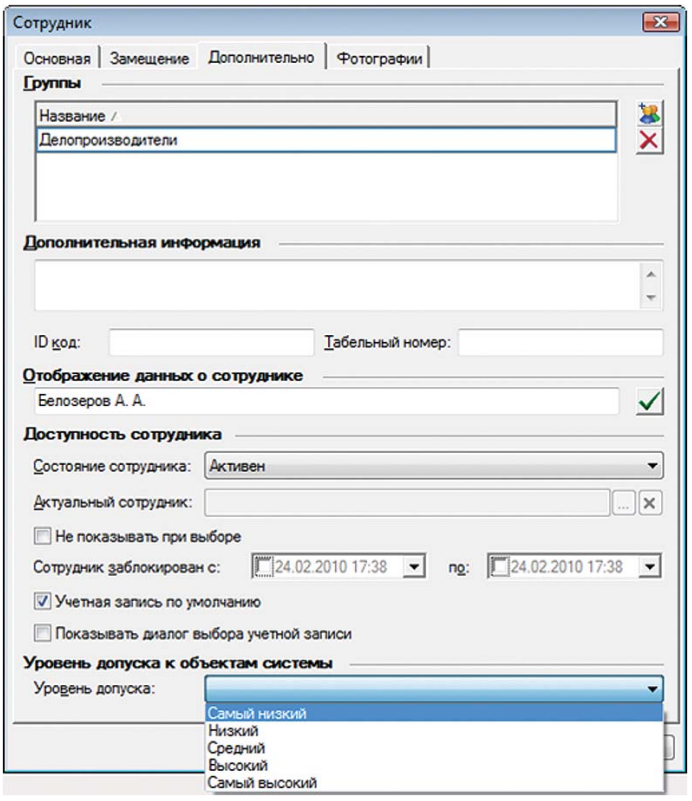

Рис. 1. DocsVision позволяет настроить специальную структуру папок, матрицы безопасности и уровень доступа к документам, благодаря которым точно регламентировано, с какими папками и документами работает сотрудник.

живать изменения, дополнения и правки, которые вносятся другими сотрудниками. При этом исключается потеря информации: это достигается за счет применения политики, заключающейся в том, что при согласовании договоров и других документов, правки сотрудников вносятся в виде замечаний к документу, но сделать исправление может только один человек. При утверждении документа пользователи видят ту версию документа, которая окончательно согласована и в нее не были внесены коррективы, мешающие принятию решения.

Дополнительно защита информации обеспечивается применением стандартных мер безопасности при удаленной работе, например с использованием VPN-тоннелей, HTTPS- протоколов и ЭЦП.

Подводя итог, отметим, что перечисленные выше возможности позволяют защитить сами документы, но делать это необходимо комплексно:

1. DocsVision позволяет настроить специальную структуру папок, матрицы безопасности и уровень доступа к документам, благодаря которым точно регламентировано, с какими папками и документами работает сотрудник (рис. 2).

2. Кроме этого, можно настроить систему ролей доступа к документам, доступ к справочной информации и поисковым фильтрам, которые также помогают в ограничении прав использования документов. Можно также не продумывать сложную структуру папок, например, настроить для папок такие фильтры поиска, что сотрудник, открывающий ее, будет видеть только те файлы, автором которых он является. Данный способ организации защиты информации позволяет сотруднику работать только с нужными ему документами. Сотрудник не видит документы своих коллег, пока они находятся в работе, но, как только документ перейдет в стадию действующего, с ним сможет ознакомиться большее количество сотрудников – как делопроизводители, так и те сотрудники, которые имеют права на доступ к уже готовому документу.

3. Дополнительно в версии DocsVision 4.5 введен модуль "Конструктор решений", который позволяет усилить ролевую модель безопасности: пользователи включаются в бизнес-процесс и в ходе работы им приходят карточки документов с определенными данными. Пользователь, в зависимости от заданной роли, будет видеть только ту информацию, которая доступна ему в рамках данной роли. Таким образом, исключаются те данные, которые не нужны простым пользователям (роли исполнителя и делопроизводителя). Также данный метод позволяет исключить реквизитную часть документов для руководителей компании, коммерческого и юридического департаментов.

4. В дополнение к возможностям системы DocsVision можно использовать сторонние продукты, которые дают возможность контролировать документооборот за пределами организации и позволяют настроить такие сценарии, как запрет печати документов из системы, даты, в рамках которых действуют полномочия сотрудника на работу с документом, исключается возможность отправки документа по электронной почте. Одним из таких продуктов является служба управления правами Microsoft Windows Rights Management Server, реализованная в виде службы Windows Server 2008. Таким образом, обеспечить защиту от потери данных в рамках работы с документами внутри организации, можно с помощью возможностей системы DocsVision, а для исключения утечек информации за пределы компании, необходимо использовать сторонние продукты и приложения.

Примеры реализаций

Компания Digital Design, партнер компании "ДоксВижн", реализовала ряд проектов по защищенному документообороту. Среди компаний-заказчиков: группа компаний Финам – один из крупнейших инвестиционных холдингов России; инвестиционно-финансовая компания "Алемар", специальный депозитарий "Инфинитум"; управляющая компания "Металлоинвест", ФГУП Морское конструкторское бюро "Алмаз" и др.

В качестве примера интеграции системы DocsVision с системой Microsoft Windows Rights Management Server можно привести проект, реализованный в компании "Транспрофконсалт", основной деятельностью которой является оказание юридических и консалтинговых услуг в области ведения судебных дел. В рамках проекта были автоматизированы ключевые процессы документооборота, включая маршрутизацию документов, импорт и экспорт судебных дел. Для разграничения прав доступа к документам был использован инструмент Windows Rights Management Server, дополнивший стандартную функциональность системы DocsVision.

Выше была рассмотрена возможность построения защищенного документооборота с функцией контроля изменений, вносимых в документ. На базе данной модели специалистами компании Digital Design была реализована защита документов в СЭД компании "Центральный Телеграф". Компания предоставляет высокоскоростной доступ в интернет, услуги передачи данных, подключение банкоматов и POS-терминалов и др. Внедренная в компании "Центральный Телеграф" система DocsVision позволяет обеспечить хранение файлов и информации карточек электронных документов, управлять правами доступа и иерархией папок архива электронных документов. Также система позволяет осуществлять контроль совместного доступа пользователей к карточкам и электронным документам с запретом одновременного редактирования несколькими пользователями объектов системы.

Вместо заключения

Рассмотрев способы организации защищенного документооборота в системе DocsVision, можно сделать вывод: полноценная защита документооборота внутри и за пределами организации возможна лишь при проведении комплекса работ по защите информации: разграничение прав доступа, дополнительные папки, ролевая модель, учетные записи пользователей, мандатная безопасность, дополнительные средства защиты от утечек информации за пределы организации.

Компания Digital Design, в дополнение к использованию стандартных средств защиты, предлагает свои услуги в качестве специалиста в области создания систем защищенного электронного документооборота. СЭД – это не только платформа DocsVision, это – комплекс работ и систем, в который входят: создание инфраструктуры, внедрение системы электронного документооборота, подготовка к аттестации системы на соответствие 152-ФЗ, обучение специалистов заказчика.

Евгений Макаревич,
руководитель проектов департамента управления информацией компании Digital Design