Г. А. Шелеляева
г. Гомель, ГГУ им. Ф. Скорины

ЗАЩИТА ИНФОРМАЦИИ В ЦИФРОВОЙ СРЕДЕ

Процесс информатизации хозяйственной деятельности меняет традиционные взгляды на совершение многих коммерческих операций. На сегодняшний день в нашей стране остается все меньше сфер экономики, в которых бы не использовались высокие технологии. Бизнес в настоящее время является наиболее динамичным и оперативным участником рынка. Все большее количество коммерческих операций совершается в цифровой среде. Для этого в Республике Беларусь создаются все предпосылки как на законодательном, так и на технологическом уровне. Однако наибольшей проблемой по-прежнему остается защита информации при совершении коммерческих операций. Соблюдение конфиденциальности коммерческой информации в цифровой среде требует иных, отличных от выработанных ранее технологий. Подходы к защите данных при заключении сделок в настоящее время претерпевают значительные изменения

По-прежнему основным носителем информации, сопровождающим все бизнес-процессы, остается документ. Документ – это совокупность трех составляющих: носитель; форма; активизация определенной деятельности. Именно некоторая деятельность и превращает данные в документ. Но документ перестает существовать, если в дальнейшем не подразумевает процедуры обработки. Форма документа тесно связана с характером дальнейшей деятельности, она порождает необходимость документов. При этом не существенен носитель информации, бумажный или электронный документ играют одинаковую роль в бизнес-процессах.

В Республике Беларусь принят и успешно реализуется закон «Об электронном документе и электронной цифровой подписи», согласно которому «подлинный электронный документ приравнивается к документу на бумажном носителе, подписанному собственноручно, и имеет одинаковую с ним юридическую силу». Электронные документы позволяют переместить центр тяжести компьютерной технологии с традиционных структурированных алфавитно-цифровых данных на потоки данных, дополненные большими объемами неструктурированного текста, изображений, звука, видео и графики. Такие документы смогут также включать гипертекстовые связи, переработанные OLE – объекты, текстовые объекты и реляционные данные. Электронный документ будет ограничен такими параметрами как его содержимое, структура данных, форматы и стандарты режима передачи и, самое важное, характер его использования. При изменении любого из этих параметров соответственно будет меняться документ. Он будет открытым, гибким, адаптируемым, многомерным.

За несколько лет концепция электронного документа получила свое развитие от обычного графического образа документа до идеи управления документами. Сегодня документ – это форма знакомого вида, обработка которой происходит с помощью последовательного применения тесно взаимосвязанных технологий в рамках так называемых Систем Управления Электронными Документами (СУД) или Electronic Document Management Systems (EDMS). Огромный управленческий эффект в самой ближайшей перспективе сулит переход от электронного документооборота в отдельных локальных офисных сетях к единой системе документооборота территориально распределенной системы организаций, которую можно с точки зрения документооборота рассматривать как один единый виртуальный офис. Электронный документооборот в коммерческой деятельности – это, в первую очередь, возможность (и необходимость) свободного обмена данными и документами с партнерами по бизнесу. Следовательно, любой недобросовестный партнер может получить доступ и к внутренней конфиденциальной информации предприятия.

Важно заметить, что в условиях активного перехода к электронному документообороту бумажный документооборот продолжает, и в обозримом будущем будет продолжать оставаться значимой составляющей документооборота. Следовательно, в этих условиях всегда будет возникать проблема одновременного управления бумажным и электронным документооборотом, сохранения целостности данных, защита их от несанкционированного использования и модификации. В общем случае один и тот же документ может в течение всего своего жизненного цикла существовать в электронном и бумажном виде, причем иногда одновременно могут существовать бумажные и электронные экземпляры одного и того же документа. Таким образом, разделение контроля за бумажными и электронными документами вносит путаницу и, в конечном счете, приводит к потере контроля за документооборотом предприятия в целом. Главная задача здесь – естественным образом, в рамках единой системы, обеспечить контроль над всеми ипостасями документа, а также защиту информации независимо от ее носителя.

Именно электронный документ является основной угрозой информационной безопасности корпоративных систем. Большинство производственных процессов на объектах промышленности автоматизированы и объединены в рамках корпоративной информационной системы, которая обрабатывает и хранит информацию, управляя работой техники. Необходимость постоянного общения с партнерами требует, чтобы корпоративная система имела открытый доступ к Интернету. Подобная схема отвечает реалиям и воспринимается как объективная необходимость, однако руководители предприятий в связи с этим пока не очень задумываются об обеспечении информационной безопасности возглавляемого ими предприятия. Забывая при этом, что и само производство, и информация – к примеру, особенности технологического процесса – могут являться объектом пристального внимания со стороны конкурентов. Ситуация усугубляется быстрым ростом популярности в корпоративной среде концепции BYOD (bring your own device – «используй свое собственное устройство»). По статистике, в США и Европе уже две трети компаний допускают подключение к своей инфраструктуре личных мобильных

устройств сотрудников. В результате понятие «офис» становится виртуальным и распространяется далеко за пределы помещения. Доступ к IT-инфраструктуре компании получают сотрудники, работающие на выезде, филиалы, удаленные работники и так далее [1]. В таких условиях возрастает риск потери или хищения данных, составляющих коммерческую тайну и усиливается значимость технологий защиты информации. Требование обеспечения защиты данных в большинстве систем выполняется за счет традиционных средств парольной защиты, разграничения доступа, межсетевой и антивирусной защиты. Вместе с тем, анализ показывает явную недостаточность этих средств, так как они не учитывают наличие человеческого фактора – инсайдерной опасности, наличие таких каналов утечки информации как случайный несанкционированный доступ, перехват электронных документов, передаваемых по каналам связи и т. п.

По данным [2], исследовательская служба российского HR-портала HeadHunter провела опрос среди работников компаний и выяснила, что более половины из них при увольнении забирают с собой рабочие, в том числе конфиденциальные корпоративные данные. 37 % опрошенных признались, что копировали и уносили собственные наработки, 19 % – уникальные методики и разработки, созданные в команде, 11 % – базы данных с контактами клиентов и деловых партнеров, 6 % – результаты труда своих коллег, а 3 % – любые конфиденциальные сведения. Как отмечают ряд исследователей, [3], использование парольной аутентификации в информационных системах предприятий и организаций себя изживает. Продолжая применять эту традиционную методику доступа в отношении собственных информационных ресурсов, предприятия фактически ставят под угрозу эффективность, а, иногда, и само существование предприятия.

Наиболее уязвимыми составляющими бизнес-среды являются каналы передачи данных, электронная почта, бизнес-приложения. Нарушения нормального функционирования бизнес-процессов приводят к экономическим потерям при ведении электронной коммерции, наносится ущерб имиджу и репутации компании. С целью снижения рисков больших финансовых потерь предприятия должны инвестировать средства в инструменты обеспечения безопасности и эти инструменты тем действеннее, чем реже они используются в бизнес-сообществе.

Помимо традиционных дешевых, появляется ряд средств, представляющих интерес именно для систем электронного документооборота. К таким средствам относится, в первую очередь двух- и многофакторная аутентификация. Она основана на совместном использовании нескольких факторов аутентификации (знаний, средств или объектов хранения одной из информационных составляющих легитимной процедуры аутентификации), что значительно повышает безопасность использования информации со стороны пользователей, подключающихся к информационным системам по защищенным и незащищенным каналам коммуникаций.

Все методы многофакторной аутентификации сложны в использовании или требуют применения дополнительного программных или аппаратных средств. Громоздкость таких методов оправдывается их хорошей защищенностью в том числе и от пользователей, предпочитающих так называемые «слабые пароли». Немаловажным является и то, что двух- или многофакторная система аутентификации позволит осуществлять коммерческие операции, используя мобильные устройства, объединить коммерческую и банковскую деятельность, реально обеспечить информационную безопасность пользователя электронных услуг.

Список использованных источников

1 Компьютерные вести [Электронный ресурс]. – Режим доступа : http://www.kv.by/category/tegi/zashchita-informatsii. – Дата доступа : 10.05.15.

2 Компьютерные вести [Электронный ресурс]. – Режим доступа : http://www.kv.by/content/zashchita-informatsii-vblizi. – Дата доступа : 24.03.15.

3 Компьютерные вести [Электронный ресурс]. – Режим доступа : http://www.kv.by/content/kak-raspoznat-insaidera. – Дата доступа : 03.03.15.