ПРОБЛЕМЫ СОХРАННОСТИ И БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ И СОВРЕМЕННЫЕ СПОСОБЫ ИХ РЕШЕНИЯ

А. В. Коротков, компания «Тенденция»,
А. В. Холин, кандидат технических наук, ИПК МТУСИ

«Тогда лишь двое
тайну соблюдают,
Когда один из них
её не знает»
Уильям Шекспир

В современном мире информация — как личная, так и коммерческая — становится всё более и более уязвима. Конфиденциальная же информация превратилась в товар, за которым идёт охота. Значительный ущерб способна нанести не только кража, но и банальная утеря ключевых материалов документооборота (баз данных, документов, содержащих конфиденциальные сведения и других). Традиционное резервное копирование не всегда может отвечать требованиям времени по оперативности создания и восстановления копий, надёжности хранения и защите от несанкционированного доступа. Каким бы частым ни было резервное копирование, всегда остаётся вероятность сбоя и потери важных данных в промежутке между копированиями. Резервная копия на сервере компании не спасёт критические бизнес-данные, если в офисе произойдёт пожар или кража. Защиту от несанкционированного доступа на основе пароля, задаваемого администратором, ответственным за создание копий, достаточной назвать нельзя.

Все эти вопросы решаются при использовании системы хранения данных (СХД), представляющей специализированное оборудование, находящееся в корпоративной сети пользователя. Пользователь в таком случае работает с файлами непосредственно в СХД, не подвергая данные различным рискам на своей рабочей станции, а СХД, в свою очередь, обеспечивает резервирование в режиме реального времени, что обеспечивает актуальность хранимых данных на любой момент времени с заданным коэффициентом надёжности Кн=99,9. Опционально может применяться шифрование для обеспечения безопасности конфиденциальных данных.

Идея непосредственного использования и хранения чувствительных данных в шифрованном виде на специально выделенных файловых серверах — не нова. Сегодня на рынке представлен ряд предложений, которые позволяют любой организации приобрести необходимое клиентское и серверное ПО для развёртывания сетевого хранилища и организации групповой работы с чувствительными данными. Это, как правило, некое клиент-серверное приложение, для внедрения и поддержки которого требуются значительные материальные затраты: приобретение самого ПО, выделение дополнительной вычислительной техники, оплата квалифицированного ИТ-персонала, получение в дальнейшем новых версий ПО от производителя, затраты на обучение персонала пользованию новыми пакетами программ и другие. Если крупным предприятиям, имеющим специализированные отделы и департаменты информационных технологий, эти материальные и трудовые затраты по плечу, то для компаний малого, а то и среднего бизнеса внедрение подобных систем может оказаться неоправданно трудоёмким и экономически нецелесообразным. Неудивительно, что в этом сегменте организаций системы защищённого хранения конфиденциальной информации зачастую не применяются вовсе. Представляется разумным именно для таких компаний передать внедрение и поддержку подобных систем на аутсорсинг специализированной организации – провайдеру данной услуги (Data Security Provider). Выгоды очевидны: отпадает потребность в затратах на выделенные серверы, их обслуживание, настройку и поддержку ПО. Не вызывает сомнений, что компания, оказывающая подобные услуги, способна поддерживать существенно более производительные и отказоустойчивые серверы, нежели каждый из клиентов в отдельности, и обеспечить доступность данных по классу «пять девяток» (Кн=99,999).

Однако в таком случае встаёт вопрос обеспечения провайдером подобной услуги (Data Security Provider) конфиденциальности информации заказчика. Этот щекотливый вопрос может быть решён в технологическом и юридическом аспектах. В плане технологий современное развитие средств криптографии позволяет гарантировать необходимый уровень безопасности конфиденциальных данных при использовании существующих стойких шифровальных алгоритмов, в частности алгоритма шифрования ассиметричным ключом заведомо избыточной длины. При рассмотрении юридического аспекта необходимо руководствоваться нормативно-правовыми документами по защите конфиденциальной (персональной) информации в Российской Федерации, в частности «Доктриной информационной безопасности РФ», где указано, что основной угрозой информационной безопасности РФ является использование несертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации. Следовательно, применяемое криптографическое ПО должно пройти соответствующую сертификацию, а сама деятельность подобного провайдера должна быть лицензирована.

Использование услуги конфиденциального хранения информации и групповой работы над документами по схеме аутсорсинга имеет для потребителя-компании малого и среднего бизнеса следующие преимущества:

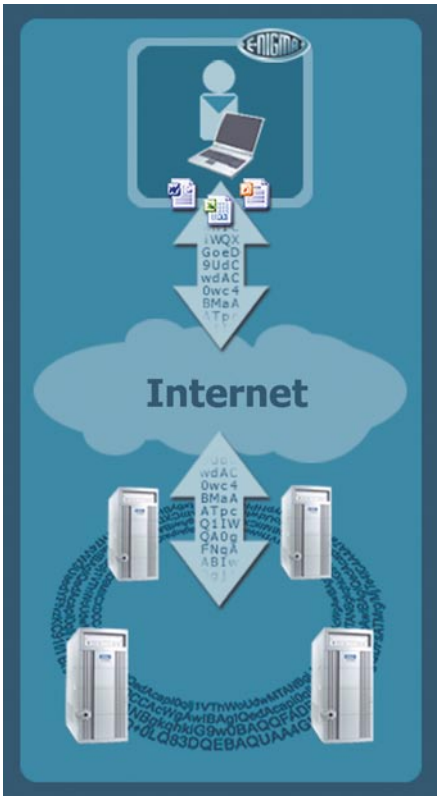
- снижение стоимости внедрения и поддержки системы на порядки: экономия на программном и аппаратном обеспечении, на ИТ-персонале;
- возможность полностью исключить потенциальную утечку конфиденциальной информации через сотрудников ИТ-подразделения, имеющих, как правило, полный доступ к любым данным, если подобная система устанавливается и поддерживается организацией самостоятельно;

- несравнимое качество и надёжность работы системы: возможности резервирования и показатели отказоустойчивости у провайдера таких услуг на порядки выше, чем у отдельной компании;

В соответствии с концепцией дистанционного высоконадёжного хранения и работы с критическими бизнес-данными российскими разработчиками был создан программный продукт E-NIGMA™ (www.e-nigma.ru).

E-NIGMA™ — система удалённого хранения конфиденциальной информации, позволяет своим пользователям свести к минимуму риски, связанные с уничтожением, утечкой, утратой, порчей всевозможных чувствительных данных, и обеспечить защищённую групповую работу над документами.

Небольшую по объёму программу клиента системы можно хранить на дискете, флэш-диске или быстро получить из Интернета. Запустив не требующее установки клиентское программное обеспечение, пользователь авторизуется на сервере по совокупности логина, пароля и ключа. Подключение происходит по 80 порту протокола TCP (популярный протокол HTTP), что гарантирует успешный доступ в любом сетевом окружении, в том числе и через прокси-сервер. Все коммуникации осуществляются исключительно в шифрованном виде. Удобный и понятный интерфейс осуществляет загрузку-выгрузку файла в удалённое хранилище, удаляя все следы присутствия конфиденциального документа на компьютере. Загруженный в систему документ в зашифрованном виде по интеллектуальному алгоритму синхронизации дублируется в массиве территориально распределённых серверов, что гарантирует сохранность, конфиденциальность и мгновенный доступ для авторизованного пользователя. В шифрованном виде хранятся также имена файлов, папок, комментарии к файлам. Все операции по шифрации/дешифрации файлов осуществляются только клиентским ПО на компьютере пользователя посредством персонального ключа. Информация пользователей, таким образом, закрыта не только для несанкционированного доступа извне, потенциальных инсайдеров внутри собственной корпоративной сети, но и для специалистов, обслуживающих массив серверов-хранилищ, размещённых на технологических площадках провайдера. Ведь все криптографические операции с данными, процедура генерации ассиметричных ключей выполняются исключительно ПО пользователя, а серверы работают в пассивном режиме, многократно дублируя массивы данных неизвестного для них содержания. Потенциальная компрометация сервера, таким образом, нисколько не отразится на данных пользователей – без ключей, хранящихся исключительно у заказчиков, хранимые данные бесполезны. В случае подозрения на компрометацию ключа пользователя (например, неадекватное хранение), он может быть оперативно заменён. Но, разумеется, только в случае предоставления верного ключа для инициирования процедуры замены – в любом другом случае доступ к данным исключён. В рамках организации возможна совместная работа с файлами посредством предоставления доступа другим членам рабочей группы.



Общая схема работы системы удалённого хранения конфиденциальной информации E-

Ключевые особенности E-NIGMA™:

Эффективное и экономичное решение проблем информационной безопасности для предприятий, особенно для малого и среднего бизнеса.

Необходимый инструмент обеспечения сохранности и целостности критически важной бизнес-информации в режиме on-line.

Интуитивная простота пользования. Программное обеспечение не требует установки. Понятные настройки создают комфортный интерфейс пользователя при высочайшем уровне безопасности и позволяют обойтись без наличия в штате компании дорогостоящих специалистов по информационной безопасности и сэкономить время и деньги на внедрении по сравнению с традиционными решениями.

Групповая работа множества сотрудников с конфиденциальными корпоративными документами из любой точки мира посредством Интернета с абсолютной уверенностью в отсутствии утечек данных. Возможность перехвата, которой подвержены традиционные решения обмена: электронная почта, FTP-серверы, обмен документами через веб-сайты, — исключена полностью.

Максимальный уровень защиты. Шифрование осуществляется с помощью криптографической библиотеки, сертифицированной для использования в электронных банковских операциях.

Автоматическое удаление следов документов, загруженных в E-NIGMA™. Защита от потери или кражи вычислительной техники. Безопасная работа с чувствительной информацией с чужих компьютеров или интернет-кафе. Встроенный файл-шреддер.

Развитие телекоммуникационной инфраструктуры, стремительный рост скорости и способов доступа к сетям передачи данных при одновременном удешевлении самого доступа – с одной стороны, и повсеместное проникновение информационных технологий во все сферы повседневной деятельности и, как следствие, рост ценности информации, хранимой в электронном виде, и потребности гарантированного оперативного и безопасного доступа к ней — с другой стороны – создают предпосылки для высокой востребованности и популярности подобной системы. Будущее развитие изложенной концепции предусматривает реализацию идей «тонкого клиента» и виртуального офиса, предоставляющих через единую точку входа безопасный доступ к рабочим данным сотрудника, интеграцию со средствами обмена сообщениями, наращивание функционала электронного документооборота.