

# InfoWatch CryptoStorage: защита конфиденциальных данных для компаний СМБ

Статья описывает развертывание системы обеспечения конфиденциальности бизнес-информации с помощью шифрования. Задача сформулирована с точки зрения небольшой компании (СМБ), нуждающейся в обеспечении безопасности рабочих документов, архивов и транзакций.

## Модельное техническое задание

Дано: компания малого или среднего масштаба, оказывающая юридические и консалтинговые услуги. В нескольких отделах (корпоративного права, гражданского судопроизводства и досудебного урегулирования, арбитражной практики и т. п.) занято 30–50 человек, в бухгалтерии — три–шесть сотрудников, руководителей (использующих преимущественно ноутбуки) — три–пять человек. Регулярно возникает необходимость организации дистанционного канала доступа к серверам локальной сети (выезжающие к клиентам консультанты, адвокаты в ходе судебных процессов и т. п.). Инфраструктура обслуживается одним системным администратором (в штате или в рамках ИТ-аутсорсинга). Сходные задачи и требования возникают и в случае обособленного юридического подразделения в структуре крупной корпорации или государственного учреждения. ИТ-оборудование представлено несколькими файловыми серверами, выделенным сервером специализированных приложений и баз данных, базовой сетевой инфраструктурой и широкополосной линией связи. В компании развернут домен Windows Active Directory, типовые политики разделения доступа к ресурсам домена для каждой рабочей группы: юристы различных отделов, руководство и бухгалтерия, дистанционные пользователи (члены этой группы работают в домене через VPN-соединение или терминальный доступ).

## Решение

Информация в наши дни обладает наивысшей ценностью. Даже биржевая цена золота, ресурса с самым высоким на сегодня уровнем доверия, определяется в итоге поступающей к трейдерам информацией. Тем более ценна юридическая информация, своевременность и полнота которой определяют судьбу коммерческих структур всех уровней.

С юристом или бизнес-консультантом, как и с лечащим врачом, следует быть полностью откровенным; иначе он не сумеет в полной мере помочь своему клиенту. Это означает, что при взаимодействии с юридическими/консалтинговыми компаниями де-факто нарушается принцип хранения наиболее важных данных в пределах сети

компании-клиента. При заключении соответствующего контракта оговариваются неустойки на случай утечки клиентских данных, однако репутационные и технологические (например, из-за утечки еще не запатентованных разработок) потери не всегда измеримы в денежном выражении и чаще всего просто недопустимы.

Становясь поверенным компании-клиента, юридическая или консалтинговая фирма принимает на себя ответственность и риски, связанные с сохранностью клиентских данных. Организовать свою информационную безопасность так, чтобы свести к минимуму техническую возможность утечки, — абсолютно необходимый шаг в данной ситуации. Полностью исключить из рассмотрения человеческий фактор и *social engineering* нельзя, но это уже забота внутренней службы безопасности. Техническую же защиту информационного периметра следует возложить на специализированное ПО — в рассматриваемом нами примере на CryptoStorage компании InfoWatch.

InfoWatch CryptoStorage — это многоцелевой инструмент, предназначенный в первую очередь для шифрования данных с целью их защиты от несанкционированного использования. Продукт ориентирован на небольшие компании и персональное использование; корпоративным клиентам предлагается более функциональная его версия InfoWatch CryptoStorage Enterprise. В последнем случае администратору продукта оказывается доступно управление финансовыми, юридическими и иными рисками, связанными с утратой данных.

Для малого или среднего предприятия наиболее предпочтительной представляется базовая версия CryptoStorage. Она обеспечивает защиту информации на компьютерах (стационарных и мобильных) и носителях (включая флэш-накопители) сотрудников, безопасный обмен данными с партнерами и клиентами, надежную сохранность информации на серверах компании и безопасный многопользовательский доступ к ней. Ключ к успеху юридической компании — доверие ее клиентов, и лишь высокий уровень безопасности данных способен стать залогом такого доверия.

Развернуть InfoWatch CryptoStorage на компьютерах юридической/консалтинговой организации для ИТ-практика не составит труда. Инсталляция выполняется в несколько простых шагов при помощи «Мастера установки» (или стандартными средствами установки в домене Windows); минимальные системные требования по современным меркам весьма скромны: 1-ГГц ЦП Intel Celeron,

256-Мбайт свободная оперативная память, 10 Мбайт на жестком диске. Поддерживаются 32- и 64-разрядные версии платформ Microsoft Windows от XP SP3 до 7 и Small Business Server 2011. Таким образом, зашифровать чувствительные данные при необходимости удастся даже на нетбуке или Wintel-планшете. Установка пакета производится с правами администратора, что при хорошей организации ИТ-инфраструктуры (когда непосредственные пользователи настольных ПК и ноутбуков не имеют администраторских привилегий) гарантирует стабильность и постоянство защиты.

Ключевой идеологией CryptoStorage выступает парадигма электронного сейфа. Пользователи могут создавать отдельные защищенные папки и так называемые контейнеры, с криптозащитой, подключаемые как виртуальные логические диски, а также шифровать разделы дисков и отсоединяемые носители целиком. Операции с перечисленными выше защищенными объектами выполняются наиболее простым и доступным способом — через контекстное меню стандартного «Проводника» Windows, появляющееся по нажатию правой клавиши мыши на выделенном объекте.

Защищенные папки CryptoStorage могут создаваться на локальных жестких дисках ПК, на отсоединяемых носителях или на других компьютерах локальной сети с файловой системой NTFS. Пока такая папка не подключена легитимным пользователем, она надежно защищает содержащуюся в ней информацию от несанкционированного доступа. Легитимными по отношению к данной папке могут выступать несколько пользователей данного ПК или локальной сети, причем у различных подкаталогов в пределах одной и той же защищенной папки могут быть различные списки доступа.

Отметим важный с точки зрения процедур внутренней безопасности момент: статус легитимного пользователя данной защищенной папки может не быть постоянным (к примеру, занимавшийся данным делом юрист переведен в другой отдел или уволен). Внутренние механизмы InfoWatch CryptoStorage предусматривают пере-

шифрование папки с применением нового ключа после удаления пользователя из списка легитимного доступа, в результате обеспечивается высокий уровень безопасности данных.

Специфическим инструментом безопасности в структуре CryptoStorage выступает контейнер — своего рода цифровой сейф фиксированного объема (не менее 12 Мбайт при форматировании под NTFS). Для нелегитимных пользователей ПК или локальной сети такой контейнер представляет собой обычный файл, который можно удалить, если к нему имеется прямой доступ, однако невозможно вскрыть, не зная пароля. Все файлы и папки внутри контейнера зашифрованы и являются защищенными.

Легитимный пользователь, подключая контейнер, получает возможность работать с ним как с дополнительным логическим диском в своей системе — форматировать, создавать и перемещать в него файлы. Здесь также поддерживается список доступа, позволяющий взаимодействовать с контейнером несколькими легитимным пользователям.

Защищенный контейнер особенно удобен в тех случаях, когда сотрудникам юридического/консалтингового предприятия приходится обмениваться конфиденциальной информацией между собой либо с клиентами по заведомо уязвимым каналам — например, по электронной почте либо через внешние Интернет-сервисы. Если на компьютерах отправителя и получателя почтовых отправок установлена система InfoWatch CryptoStorage и оба они (отправитель и получатель) включены в список легитимных пользователей контейнера, то такой контейнер в качестве надежного цифрового сейфа может быть прикреплен к самому обычному электронному письму. В результате конфиденциальную информацию окажется безопасно размещать даже на внешних Интернет-сервисах: защиту ее обеспечит криптоконтейнер.

Максимальный уровень защиты всей информации, размещенной на ПК, обеспечивается при установке InfoWatch CryptoStorage на системный раздел жесткого диска. В такой ситуации авторизация для доступа к защищенному

разделу будет выполняться до загрузки операционной системы, так что обычные трюки с обходом парольной защиты BIOS (сброс CMOS, извлечение батарейки, подключение извлеченного физического диска на другом компьютере) не позволят получить доступ к оберегаемым данным.

Безусловно, в распоряжении потенциального злоумышленника остается старый добрый метод подбора пароля «грубой силой», перебором всего доступного словаря. Однако даже с использованием самых современных процессоров «хороший» восьмисимвольный пароль (не являющийся словарным словом и содержащий небуквенные символы и буквы в разном регистре) не удастся подобрать и за десяток тысяч лет.

InfoWatch CryptoStorage при шифровании системного раздела обеспечивает защиту не только собственно файлов данных, но и файла аварийного дампа памяти и слепок состояния оперативной памяти, сохраняемого на системном диске при переходе в спящий режим. Даже получив физический доступ к такому диску, злоумышленник не сумеет восстановить зашифрованные данные.

InfoWatch CryptoStorage позволяет гарантированно удалять папки и файлы, поскольку папки и файлы, удаленные обычным способом, могут быть впоследствии восстановлены при помощи специальных утилит и информации, хранившаяся в удаленном объекте, станет доступной посторонним лицам. Функция гарантированного удаления доступна как для защищенных, так и для незащищенных объектов.

Использование CryptoStorage для защиты конфиденциальной информации оказывается необходимой для большой компании, вынужденной пользоваться ИТ-услугами по принципу аутсорсинга. Сотрудники центров технической поддержки, в руки которых попадает вышедший из строя ноутбук, командированные из других организаций или просто случайные посетители/знакомые/друзья, которыхпустили «посидеть за компьютером»; системный администратор-фрилансер все эти лица, оставаясь один на один с ПК, представляют потенциальную


угрозу для сохраняемых на нем данных. Даже в отсутствие злого умысла они способны нарушить целостность важной информации, что может обернуться абсолютно неприемлемыми репутационными потерями и для самой юридической/консалтинговой фирмы, и для ее клиентов.

Если на компьютере с установленной системой InfoWatch CryptoStorage запущена подсистема «Защищенные логические диски», то отсутствует доступ к указанным выше защищенным разделам диска. Кроме того, пространство, занимаемое ими на диске, невозможно использовать. Утилита восстановления дисков позволяет сделать это пространство снова доступ-

ным для использования, в том числе и для InfoWatch CryptoStorage. Безвозвратно удалить с компьютера можно любой файл или папку, нажав в контекстном меню Гарантированно удалить, причем файл, удаленный таким образом, в дальнейшем уже не восстановить никакой утилитой.

В число основных преимуществ InfoWatch CryptoStorage входят, таким образом, надежность защиты, которую обеспечивают высокая компетенция компании-разработчика и современные стойкие алгоритмы защиты данных, простота и удобство использования (наглядность интерфейса, легкость установки и настройки), высокая производительность (прозрачный

для пользователя режим работы с оберегаемыми данными, при котором все операции шифрования выполняются в оперативной памяти ПК), низкие системные требования.

Испытательная версия CryptoStorage дает потенциальным заказчикам и их клиентам шанс ознакомиться со всеми возможностями продукта, ограничивая лишь длину пароля для защищаемых объектов, — 1 символ. Гибкая же система ценообразования позволяет обеспечить покупателей достаточным числом лицензий за разумные деньги, предоставляя в их распоряжение надежный и простой в обращении криптографический инструментарий — электронные сейфы. 

**с 15 по 15**

### Экология

Компания ARBYTE ([www.arbyte.ru](http://www.arbyte.ru)) представила концепцию Green IT на конференции «Green IT. Информационные технологии и планета Земля». Как отмечают представители компании, формирование этой концепции началось в 2004 г. с решения проблемы акустического шума ПК и графических станций. В процессе исследования этой проблемы и консультаций с медицинскими специалистами компания пришла к выводу, что шум от настольных систем имеет прямые негативные последствия для бизнеса, поскольку он влияет не только на здоровье работников, но и на их трудоспособность. Был разработан ряд технических решений, позволяющих снизить уровень шума до минимальных величин. Решение стало известно как «Тихая революция. Экологичные технологии ARBYTE». Сотрудничество с кафедрой акустики МГУ им. М. В. Ломоносова по измерению шума, создаваемого системами, начавшись в 2004 г., ведется и поныне. Следующим шагом стало введение в 2005 г. пятилетней гарантии оборудования ARBYTE. В 2006 г., после вступления в силу директивы RoHS, ARBYTE активно присоединилась к международному стандарту, жестко отслеживая поставку соответствующих компонентов. Правильная утилизация — один из важнейших элементов охраны окружающей среды. В компьютерной технике содержится хороший запас вторичного сырья, ценные компоненты также возвращаются в производство. Кроме того, в России утилизация компьютерной техники для организаций — обязательная процедура, нарушение которой ведет к административной ответственности. ARBYTE наладила отношения с компаниями по утилизации оборудования. В случае покупки оборудования ARBYTE вышедшая из использования техника клиента утилизируется компанией бесплатно. Не последний элемент ARBYTE Green IT — снижение энергопотребления систем с помощью программного продукта ARBYTE Power Manager. Повышенное энергопотребление не только связано с дополнительными расходами на электричество, но и приводит к перегрузке электрических сетей и затратам на кондиционирование помещений. По результатам тестирования эффект от использования ARBYTE Power Manager составил

от 1000 до 2000 руб. на один ПК в год, что соответствует экономии в среднем 500 кВт·ч на один ПК в год. ARBYTE Power Manager будет поставляться в составе всех ПК и серверов ARBYTE в III квартале 2011 г.

### Программы

Компания NETGEAR ([www.netgear.ru](http://www.netgear.ru)) объявила о выпуске новой версии встроенного ПО для сетевых хранилищ ReadyNAS. В версии «прошивки» 4.2.18 обеспечивается совместимость с 3-Тбайт жесткими дисками, появилась возможность расширения массивов в режиме Flex-RAID (в том числе RAID 10 в режиме Flex-RAID), улучшены возможности управления средствами X-RAID2, добавлены функции восстановления целевого ресурса iSCSI в менеджере резервного копирования встроенного интерфейса, поддержка протокола IPv6 (в CIFS и FTP), доработаны режимы объединения каналов, включая дополнительные настройки для коммутаторов в режиме IEEE 802.3 и т. д.

### Безопасность

Компания «Антивирусный Центр» ([www.antiviruspro.com](http://www.antiviruspro.com)) объявила о выпуске решения для защиты информационных систем обработки персональных данных — типизированный пакет «Защита ИСПДн». Комплекс адресован компаниям СМБ, обеспечивает соответствие требованиям федерального закона «О персональных данных» № 152-ФЗ, содержит инструменты подготовки необходимых документов, а также обеспечивает внедрение средств защиты персональных данных. Создано несколько редакций, отличающихся составом технических средств и документов: «Защита ИСПДн STANDARD», «Защита ИСПДн PRO», «Защита ИСПДн PRO PLUS». Типовые пакеты «Защита ИСПДн» содержат набор программных средств, сертифицированных ФСТЭК, и необходимый комплект документации, которые могут быть использованы для выполнения основных требований ФЗ-152. Выбор того или иного решения зависит от задач, выполняемых в системе обработки ПДн, и от архитектуры локальной сети компании.