УДК 004.056.5 + 005.92 + 002:004.056

ПРОБЛЕМЫ ДЕЦЕНТРАЛИЗАЦИИ ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА НА ПРЕДПРИЯТИИ

Л.В. Астахова, В.С. Лужнов

В условиях интенсивного информационного развития общества все острее становится проблема перехода от бумажного к электронному хранению документации на предприятиях. Особенно актуальны эти вопросы в отношении информации ограниченного доступа. В статье рассмотрены основные проблемы децентрализации процессов хранения и обработки информации ограниченного доступа, связанные с ее конфиденциальностью, целостностью и доступностью, а также возможные направления деятельности предприятий по их устранению в контексте информационной безопасности.

Ключевые слова: информация ограниченного доступа, хранение, обработка, децентрализация.

В условиях информационного общества каждое предприятие, независимо от масштабов и форм осуществляемой деятельности, активно использует системы информатизации и автоматизации. В особенности это касается применения компьютерных систем для обработки и хранения информации. Активный рост рынка систем электронного документооборота [1] и государственные инициативы, направленные на адаптацию законодательства под современные тенденции [2], подтверждают, что потребность в переходе от бумажного к электронному хранению документации на предприятиях становится все острее.

При этом наиболее частым решением в качестве технической реализации выступает централизованное хранение всей информации предприятия на специально выделенном компьютерном комплексе (сервере). Очевидно, что при такой организации все процессы, связанные с хранением и обработкой информации, становятся зависимыми от качества работы комплекса. Его полный или частичный выход из строя может нанести значительный ущерб всему предприятию в целом.

Другой фактор, связанный с информатизацией процессов функционирования, выражается в экспоненциальном росте объемов генерируемой предприятием информации. Потребность в долгосрочном хранении больших объемов электронных данных и необходимость обезопасить деятельность от зависимости процессов от стабильности работы технических средств приводят к тому, что предприятия заменяют централизованную форму хранения и обработки информации на децентрализованную. Особенно актуальной децентрализация становится в случаях, когда информационные ресурсы распределены территориально.

В статье рассмотрены основные проблемы децентрализации процессов хранения и обработки информации и возможные направления деятельности предприятий по их устранению в контексте информационной безопасности.

Согласно стандартизированному подходу к определению информационной безопасности [3, 4], процесс по обеспечению состояния защищенности подразумевает обеспечение конфиденциальности, целостности и доступности информации. Исходя из этого, а также с учетом оговоренных негативных сторон децентрализации хранения и обработки информации, проблемы децентрализации можно разделить на следующие группы:

- нарушающие конфиденциальность информации;
- нарушающие целостность информации;
- нарушающие доступность информации.

К нарушающим конфиденциальность информации относятся следующие проблемы.

1. Отсутствие регламентов распределенного доступа сотрудников к информационным ресурсам.

В данном случае речь идет о технической сложности реализации регламентов доступа отдельных сотрудников к информации, которая необходима им для осуществления своей деятельности. Отсутствие централизованного хранилища информации ведет к необходимости производить регламентацию доступа на каждом сегменте (сервере, автоматизированном рабочем месте)

децентрализованной системы хранения и обработки, а также обеспечивать идентичность этих регламентов на всех сегментах.

В качестве возможного решения указанной проблемы могут быть использованы программные средства, предназначенные для синхронизации регламентов и политик доступа к информационным ресурсам между несколькими компьютерными системами. Зачастую о существовании подобных программных продуктов специалисты предприятия могут быть не осведомлены. Такие средства, как Novell Identity Manager и SvolReplicate, позволяют осуществлять одновременную репликацию политик и регламентов доступа сотрудников в децентрализованных системах без привязки к конкретному хранилищу.

2. Ведение журналов доступа к информационным ресурсам.

Потребность в мониторинге за доступом к информационным ресурсам с целью выявления несанкционированных попыток получить ту или иную информацию в централизованных хранилищах решается достаточно просто. В случае же с децентрализованными системами невозможно обеспечить оперативный контроль. Для решения данной проблемы невозможно продолжать использовать обычные средства (такие, как журналирование доступа и подобные). Повышение оперативности реагирования может быть достигнуто внедрением систем электронного оповещения о несанкционированных операциях. В условиях децентрализованных систем такие решения в режиме реального времени ведут автоматический учет всех событий, связанных с доступом к информационным ресурсам, и производят оповещение ответственных лиц независимо от их расположения в системе. Это достигается путем доставки уведомлений до всех сегментов децентрализованной системы с поиском назначенного получателя.

3. Защита каналов связи.

При эксплуатации централизованных систем хранения и обработки информации защита каналов связи подразумевает защиту канала «клиент – сервер» и реализуется чаще всего средствами асимметричного шифрования с выдачей электронных подписей. При переходе к децентрализованной системе появляется необходимость в защите каналов между каждым из сегментов системы, что приводит к невозможности полноценного использования централизованного шифрования в связи с отсутствием управляющего звена, выполняющего роль удостоверяющего и распределяющего данные центра. Техническая реализация шифрования при увеличении количества сегментов системы становится экономически невыгодной. Для решения данной проблемы возможно применение программных средств шифрования информации, сопровождаемых дополнительными хранилищами информации о ключах и подписях, принадлежащих соседним сегментам. Применение таких решений позволяет осуществлять защищенный обмен информацией между сегментами децентрализованной системы без необходимости в управляющем сегменте. В качестве примера может быть приведено совместное использование таких программных средств, как PGP (для шифрования), дополнительного сетевого протокола cjdns для одновременного обмена данными между сегментами и динамического хранилища данных (программный аналог технологии RAID) RLanStorage.

4. Сочетание централизации и децентрализации процессов обеспечения кадровой безопасности.

При децентрализации хранения и обработки информации ограниченного распространения на предприятии проблема кадровых уязвимостей информационной безопасности становится более острой, чем при централизованном варианте. Увеличение числа лиц, допущенных к защищаемой информации, требует организации более системной работы с ними, усиления проверочных мероприятий при приеме сотрудников на работу и мониторинга их компетенций и лояльности к организации в процессе деятельности, а также при увольнении. Для предотвращения утраты и утечки информации ограниченного доступа столь же системный характер должна иметь работа специалиста по защите информации по повышению осведомленности персонала организации в области информационной безопасности [5]. Целесообразно сочетать централизованный и децентрализованный подход к этой деятельности.

В частности, при внесении изменений в процессы функционирования организации основной задачей является подробное и четкое документирование этих изменений, а именно: фиксирование в должностных инструкциях новых обязанностей и условий для работников; формирование технической документации, отражающей формы и порядок взаимодействия с информационной

системой организации в условиях децентрализации. Кроме того, в рамках организационных мер необходимо провести инструктаж сотрудников, непосредственно осуществляющих работы с информационной системой или имеющих отношение к ее обслуживанию.

Основной проблемой, нарушающей целостность информации, является сама структура децентрализованного хранения – отдельный сегмент системы может не иметь прямого доступа к необходимой информации, так как она хранится на другом сегменте, который в данный момент может быть недоступен. Ситуация усугубляется, если целостный массив данных намеренно делится на составляющие части, которые хранятся на отдельных сегментах, и для доступа к информации необходимо произвести ее восстановление из таких частей.

Наиболее простым решением данной проблемы является реализация избыточности хранимой на сегментах информации. Суть данного решения заключается в распределении между сегментами частей информации, хранимой на соседних сегментах. Даже при выходе из строя сегмента, хранящего необходимую информацию, имеется возможность восстановить ее из распределенных частей остальных сегментов системы. Реализация такого решения заключается в применении программно-аппаратного комплекса из программного обеспечения, ответственного за репликацию (например, программный комплекс Germes), и аппаратной части в виде дополнительных физических носителей информации, не зависящих от информации, обрабатываемой на субъекте (например, параллельное включение дополнительного жесткого диска через контроллер, поддерживающий протокол CIFS аппаратно).

Проблемы, нарушающие доступность информации, в общем виде могут быть сформулированы следующим образом:

- невозможность доступа к информации, хранящейся в одном экземпляре на сегменте, который вышел из строя;
- невозможность контроля изменений информации, производимых на сегменте;
- невозможность восстановления предыдущего состояния информационного ресурса;
- потребность в осуществлении контроля за ходом создания и обработки информации.

В текущих реалиях развития информационных систем указанные проблемы доступности актуальны и для централизованного хранения, однако при децентрализации они приобретают гораздо больший масштаб и потенциально могут нанести существенный ущерб.

Для решения перечисленных проблем предлагается использование системы управления версиями (VCS). Система управления версиями позволяет хранить несколько версий одного и того же документа, при необходимости возвращаться к более ранним версиям, определять, кто и когда сделал то или иное изменение, и многое другое.

Такие системы наиболее широко используются при разработке программного обеспечения для хранения исходных кодов разрабатываемой программы. Однако они могут с успехом применяться и в других областях, в которых ведётся работа с большим количеством непрерывно изменяющихся электронных документов.

В стандартном режиме работы использование системы управления версиями подразумевает наличие центрального сервера, на котором хранится массив данных (в терминах VCS – репозиторий) [6]. Пользователи вносят изменения в документы на своих локальных рабочих местах и отправляют информацию об этих изменениях в репозиторий. При этом сохраняется возможность вернуться к любому исходному состоянию и проконтролировать доступ отдельных пользователей.

Для организации децентрализованной системы управления версиями может быть использована система Mercurial. Ее отличительной особенностью является поддержка децентрализованной работы с репозиториями и управление местами хранения разных репозиториев (распределение информации по сегментам).

Mercurial является распределенной (децентрализованной) системой контроля версий. Это означает, что рабочий процесс, как правило, выглядит следующим образом.

1. На личном компьютере создается новый репозиторий (путем клонирования существующего репозитория, создания нового и т. п.).
2. В рабочей директории данного репозитория изменяются / добавляются / удаляются файлы.
3. Выполняется фиксация изменений в данный репозиторий (то есть в локальный репозиторий на личном компьютере).

4. Шаги 2 и 3 повторяются столько раз, сколько необходимо.

5. При необходимости производится синхронизация изменений с другими репозиториями: забираются чужие наборы изменений и/или отдаются собственные.

Вся повседневная работа происходит в локальном репозитории, а при возникновении необходимости производится отправка результатов своей работы в один или несколько других репозиториев. Количество шагов при работе с отдаленными репозиториями можно сократить, если настроить Mercurial на автоматическую отправку изменений в другие репозитории при выполнении фиксации. Применение такой системы устраняет зависимость процессов хранения и обработки от какого-либо сегмента и дает дополнительные возможности по созданию различных политик и регламентов доступа отдельных пользователей системы к информации.

Описанные проблемы децентрализации процессов хранения и обработки информации постепенно становятся актуальными для все большего числа предприятий. Предложенные направления по решению указанных проблем предполагают возможность с минимальными для предприятия экономическими затратами и достаточным уровнем эффективности осуществить переход к децентрализованным системам с возможностью максимально обезопасить свои информационные ресурсы и бизнес-процессы, связанные с информатизацией деятельности.

Литература

1. СЭД (Рынок России). – М.: Аналитическое агентство TAdviser, 2012. – http://www.tadviser.ru/ index.php (дата обращения: 27.02.2014).

2. Приказ № 360 «Об утверждении Административного регламента предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по подтверждению подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей» от 28.12.2011 / Министерство связи и массовых коммуникаций РФ. – http://www.consultant.ru/document/cons_doc_LAW_127433 (дата обращения: 27.02.2014).

3. Домарев, В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – Киев: ООО ТИД «ДиаСофт», 2008. – 992 с.

4. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. – http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=STR;n=15607 (дата обращения: 27.02.2014).

5. Астахова, Л.В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации / Астахова Л.В. // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2013. – Т. 13, № 1. – С. 79–83.

6. Контроль версий с использованием Git. – М.: Регион. финансово-экономич. ин-т: Бизнес-Школа информ. технологий. – http://it.rfei.ru/~13 (дата обращения: 27.02.2014).

Астахова Людмила Викторовна, д-р пед. наук, профессор, профессор кафедры «Безопасность информационных систем», Южно-Уральский государственный университет (г. Челябинск), lvastachova@mail.ru.

Лужнов Василий Сергеевич, студент кафедры «Безопасность информационных систем», Южно-Уральский государственный университет (г. Челябинск), ua9stz@gmail.com.

Поступила в редакцию 28 марта 2014 г.

Bulletin of the South Ural State University
Series "Computer Technologies, Automatic Control, Radio Electronics"
2014, vol. 14, no. 3, pp. 107–111

PROBLEMS OF DECENTRALIZATION OF STORAGE AND PROCESSING OF INFORMATION OF LIMITED ACCESS AT THE ENTERPRISE

***L.V. Astakhova**, South Ural State University, Chelyabinsk, Russian Federation, lvastachova@mail.ru,*
***V.S. Luzhnov**, South Ural State University, Chelyabinsk, Russian Federation, ua9stz@gmail.com*

The problem of transition from paper to electronic storage of documents at the enterprises becomes very important in conditions of intensive development of the information society. Especially these questions are relevant in relation to information of limited access. The basic problems of decentralization processes of storage and processing of information with limited access were identified in article. These problems related to confidentiality, integrity and availability. The authors suggest possible directions of activity of enterprises for their elimination in the context of information security.

Keywords: information of limited access, storage, processing, decentralization, protection of the information.

References

1. *SED (Rynok Rossii)* [The ERMS (Russian Market)]. Available at: http://www.tadviser.ru/index.php (accessed 27 February 2014).

2. *Prikaz № 360 «Ob utverzhdenii Administrativnogo reglamenta predostavleniya Ministerstvom svyazi i massovykh kommunikatsiy Rossiyskoy Federatsii gosudarstvennoy uslugi po podtverzhdeniyu podlinnosti elektronnykh tsifrovykh podpisey upolnomochennykh lits udostoveryayushhikh centrov v vydannykh imi sertifikatakh klyuchey podpisey» ot 28.12.2011* [Order № 360 «On Approval of Administrative Regulation for the Ministry of Communications and Mass Communications of the Russian Federation State Services in Confirmation of the Authenticity of Electronic Digital Signatures of Authorized Persons of Certification Centers in Key Certificates Issued by them Signatures on 28.12.2011]. Available at: http://www.consultant.ru/document/cons_doc_LAW_127433 (accessed 27 February 2014).

3. Domarev V.V. *Bezopasnost' informacionnyh tehnologij. Sistemnyj podhod* [Security of Information Technologies. Systematic Approach]. Dia Soft Publ., 2008, 992 p.

4. *GOST R ISO 7498-2-99. Informacionnaya tehnologiya. Vzaimosvjaz' otkrytykh sistem. Bazovaya etalonnaya model'. Chast' 2. Arhitektura zashhity informatsii* [State Standard 7498-2-99. Information Technology. Open Systems Interconnection. Basic Reference Model. Part 2. Architecture of Information Protection]. Available at: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=STR (accessed 27 February 2014).

5. Astakhova L.V. [Problem of Identification and Assessment of Human Vulnerability of Information Security of Organization]. *Bulletin of the South Ural State University. Ser. Computer technology, Control, Radioelectronics*, 2013, no.1, pp.79–83. (in Russ.)

6. *Kontrol' Versiy s Ispol'zovaniem Git* [Version Control Using Git]. Available at: http://it.rfei.ru/~13 (accessed 27 February 2014).

Received 28 March 2014