ERP-СИСТЕМА: ПРИКЛАДНАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Шония О., Цомая Н.
Грузинский Технический Университет

Резюме

Подробно рассмотрена прикладная безопасность и защита электронных документов ERP-систем. Приведён и проанализирован один из механизмов ERP-систем - Central User Administration (CUA) для централизованного управления пользователями и их полномочиями, определены его финкции и преимущества. Для защита электронных документов в ERP-системах подробно рассмотрен интерфейс Secure Store & Forward (SSF).

Ключевые слова: Прикладная безопасность. ERP-система. Программное обеспечение. Аутентификация. Авторизация. Электронный документооборот. Цифровая подпись.

1. Введение

ERP-система (англ. Enterprise Resource Planning System — Система планирования ресурсов предприятия) — это интегрированная система на базе информационных технологий (IT) для управления внутренними и внешними ресурсами предприятия (значимые физические активы, финансовые, материально-технические и человеческие ресурсы). Цель системы — содействие потокам информации между всеми хозяйственными подразделениями (бизнес-функциями) внутри предприятия и информационная поддержка связей с другими предприятиями. Информационная система управления предприятием вообще и ERP-система в частности состоит из следующих элементов:

- модель управления информационными потоками на предприятии;
- аппаратно-техническая база и средства коммуникаций;
- СУБД, системное и обеспечивающее ПО;
- набор программных продуктов, автоматизирующих управление информацииоными потоками (ИП);
- регламент использования и развития программных продуктов;
- IT-департамент и обеспечивающие службы;
- собственно пользователи программных продуктов.

2. Основная часть

Одним из важных условием фикционирования ERP-системы является то, что она должна непрерывно работать и выполнять свои функции. ERP-система должна работать в режиме 24 часа семь дней в неделю или как минимум непрерывно в течение рабочего времени сотрудников. Ведь любой простой бизнес чреват большими издержками. Требуется обеспечить высокую степень надежности такой системы. Поскольку сегодня ни один производитель программного обеспечение (ПО) или аппаратных средств не может дать 100%-ной гарантии надежности своих решений, следует заранее предусмотреть процедуры восстановления работоспособности системы после сбоев. Необходимой частью проекта внедрения ERP является разработка стратегий резервного копирования, восстановления после сбоев, горячей замены оборудования и т. д. Все эти процедуры должны быть четко определены на момент начала продуктивного использования ERP.

Также необходимо прогнозировать объемы данных, накапливаемых в системе, для того, чтобы банальная нехватка места на диске сервера не стала причиной

прекращения работы. Итак, мы сумели заставить нашу систему надежно и непрерывно работать, но ведь ей нужно и как-то управлять. Так как ERP представляют собой сложные системы с большим количеством пользователей, то основой эффективности управления безопасностью должна служить возможность централизованно изменять параметры политики безопасности. Такими изменениями могут быть:

- создание и удаление пользователей ERP;
- присвоение прав пользователям;
- обновление ПО на клиентских компьютерах и т. д.

Часто ERP строится не как отдельная монолитная система с одним сервером приложений, а как распределенный набор отдельных систем. У каждой подобной системы существует свой набор пользователей, часто дублирующийся. Неплохо было бы в таком случае иметь средство централизованного управления пользователями и их полномочиями, и в некоторых ERP такие средства есть.

Рассмотрим в качестве примера систему **SAP R/3 (**автоматизированная система управления немецкой компании **SAP AG**, известного производителя программного обеспечения**).** В этой ERP-системе предусмотрен специальный механизм **Central User Administration (CUA)** для централизованного управления пользователями и их полномочиями. CUA позволяет выполнять следующие функции:

- унификацию учетных записей;
- назначение прав пользователям;
- ведение локальных и глобальных свойств в учетных записях.

В последнее время в ERP, так же как и во многих других комплексных программных системах, используются портальные технологии. Портал — это точка доступа к различным разнородным информационным системам. Портал также может выполнять функции аутентификации пользователей. В этом случае автоматически достигается централизация системы управления пользователями.

Раз уж мы научились эффективно управлять подсистемой безопасности ERP, то теперь можно попробовать понять, какие задачи мы сможем решить с помощью этого управления. Прежде всего, нам необходимо контролировать действия пользователей, чтобы предотвращать преднамеренные и непреднамеренные утечки информации. Очевидно, что в ERP-системах существуют различные средства контроля и аудита действий пользователей. Как на основе этих средств построить систему контроля, которая позволит узнать и предупредить утечки информации?

Для каждого конкретного проекта внедрения ERP в зависимости от текущих внутренних и внешних требований, будет спроектирована своя подсистема контроля. Попробуем выделить общепринятые этапы построения такой системы:

- Определение целей контроля и стратегии отслеживания рисков.
- Анализ рисков.
- Определение средств контроля.
- Нахождение соответствующих средств контроля для каждого из рисков.
- Мониторинг и аудит работы системы контроля.

На первом этапе определяется стратегия системы контроля, основанная на внутренних и внешних требованиях к информационной безопасности. На втором этапе составляется набор рисков, которые будут отслеживаться. На третьем этапе определяются все доступные в данной ERP-системе механизмы контроля. Для примера в SAP R/3 в качестве средств контроля может использоваться системный журнал, в который заносятся следующие события:

- открытие/закрытие сессии пользователем;
- запрос на доступ к защищаемому ресурсу;
- создание и уничтожение объекта;

- действия по изменению правил разграничения доступа.

Существуют также средства выборочного ознакомления с этой регистрационной информацией. На четвертом этапе для каждого из идентифицированных ранее рисков подбирается средство его отслеживания. Пятый этап — непосредственно эксплуатация разработанной системы контроля.

Определив прикладную безопастность можно перейти к защите электронных документов.Прежде всего, что такое электронный документ? Термин «электронный документ» не имеет никакого смысла, если в системе не используются средства электронной цифровой подписи — ЭЦП. Файл без ЭЦП — это просто файл, а не электронный документ. Конечно, в современных ERP-системах существуют интерфейсы для подключения средств ЭЦП. В SAP NetWeaver, к примеру, таким интерфейсом является **Secure Store & Forward (SSF).** Данный механизм позволяет добавлять одну или несколько цифровых подписей к любому набору данных, будь то файл или таблица в базе данных системы. Также SSF предоставляет средства для шифрования и защиты целостности данных в системах SAP. Используя возможности SSF, можно «обертывать» объекты с данными в специальные защищенные форматы (PKCS#7), перед тем как эти данные будут сохранены на отчуждаемые носители (например, дискету) или переданы по открытым каналам связи — в частности, при помощи обычной электронной почты. При этом можно конвертировать данные в безопасный формат не только для их экспорта, но и для защищенного хранения внутри системы.

Широко известна так называемая «проблема системного администратора» — как защитить информацию от системного администратора, если у него в силу его обязанностей есть все привилегии для доступа к любым данным? С помощью механизма SSF можно найти решение для этой задачи. Например, самые важные финансовые данные могут шифроваться при помощи SSF, и ключ к ним будет храниться на электронном токене только тех пользователей, которым необходима для работы данная информация. Функции SSF используют концепции цифровых подписей и так называемых цифровых конвертов для защиты электронных документов. Цифровая подпись однозначно идентифицирует того, кто поставил подпись, обеспечивает «неотказуемость» и гарантирует целостность данных. Любые изменения подписанных данных неизбежно будут выявлены при проверке подписи. Как и в случае с бумажными документами, подписанный электронный документ уже нельзя изменить. Цифровые конверты дают гарантию, что защищаемые данные будут доступны только тому, для кого они предназначены.

Итак, применение SSF для обеспечения электронного документооборота в приложениях SAP позволяет добиться следующих целей:

- гарантированной идентификации людей или компонентов, участвующих в делопроизводстве;
- «неотказуемость»;
- целостность данного документа;
- пересылки и хранения зашифрованных данных.

Использование SSF в приложениях SAP позволяет полностью отказаться от бумажных документов и подписей ручкой в пользу автоматизированного электронного документооборота, защищенного при помощи цифровых подписей и цифровых конвертов.

3. Заключение

В качестве примера использования SSF в информационных системах SAP например можно привести решение «Электронный архив», разработанное компанией «Докфлоу Бест Практис». В ноябре 2006 года компании ЛИССИ и «Докфлоу Бест

Практис» реализовали совместный проект по обеспечению поддержки ЭЦП, на платформе SAP NetWeaver. В качестве модуля генерации и проверки ЭЦП используется программный продукт LISSI-SSF. Теперь для электронного документооборота пользователи решений компании «Докфлоу Бест Практис» имеют возможность применять ЭЦП на ГОСТ-алгоритмах для подписи, проверки и шифрования электронных документов.

Литература:

1. Основы защиты сетей. Приложения и стандарты, Вильям Столлингс 2002.
2. Информационная безопасность предприятия, А. А. Садердинов, В. А. Трайнев, А. А. Федулов 2005
3. Компьютерные вирусы изнутри и снаружи, Крис Касперски 2006
4. Шония О., Цомая Н. Информационная безопасность в сетях ЭВМ. Сб.тр. ГТУ, "АСУ" №1(8), 2010
5. Шония О., Цомая Н. Политика безопасности: разработка и реализация. Сб.тр. ГТУ, "АСУ" №1(8), 2010

ERP- SYSTEM: APPLIED SECURITY AND PROTECTION OF ELECTRONIC DOCUMENTS

Shonia Otar, Tsomaia Nino
Georgian Technical University

Summary

The article discusses in details the applied security and protection of electronic documents of ERP-systems. The mechanism of ERP-systems - Central User Administration (CUA) for centrally managing users and their authority are revealed and analyzed and the functions and advantages are defined. The interface of Secure Store & Forward (SSF) is discussed for the protection of electronic documents in the ERP-system.

ERP – სისტემა: გამოყენებითი უსაფრთხოება და ელექტრონული დოკუმენტების დაცვა

ოთარ შონია, ნინო ცომაია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ERP - სისტემის გამოყენებითი უსაფრთხოება და ელექტრონული დოკუმენტების დაცვა. წარმოდგენილია და გაანალიზებულია ERP- სისტემის ერთ-ერთი მექანიზმი - **Central User Administration (CUA) (**ცენტრალური მომხმარებლის ადმინისტრირება**)** მომხმარებლისა და მათი უფლებამოსილების ცენტრალური მართვისათვის, ასევე წარმოდგენილია მექანიზმის ფუნქციები და უპირატესობები. ERP- სისტემის ელექტრონული დოკუმენტების დაცვის მიზნით დეტალურადაა განხილული Secure Store & Forward-ის (SSF) ინტერფეისი.