ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ERP-СИСТЕМ

Булдакова Т.И.[1], Коршунов А.В.[2]

В статье исследованы основные механизмы обеспечения информационной безопасности ERP–систем. Данные системы представляют собой пакет программ, предназначенный для управления, балансировки и оптимизации ресурсов предприятия, они обеспечивают общую модель данных и процессов для всех сфер деятельности предприятия. Рассмотрены основные аспекты безопасности при работе с системами, реализующими ERP–стратегию. В настоящее время для обеспечения информационной безопасности в ERP–системах, кроме штатных средств защиты информации, используются дополнительные программные средства, в том числе криптографические, чтобы выполнить все требования по информационной безопасности. Данная статья даёт структурированное представление обо всех механизмах обеспечения информационной безопасности в системах управления предприятием. Рассмотрены сетевая безопасность ERP–систем, а также безопасность на уровне базы данных, уровне сервера приложений и пользовательском уровне представления. Обсужден вопрос о предоставлении доступа пользователю на основе модели RBAC.

***Ключевые слова**: ERP–система, сетевая безопасность ERP–систем, сервер приложений, уровень представления, модель RBAC*

Введение

ERP (англ. Enterprise Resource Planning, планирование ресурсов предприятия) – это организационная стратегия интеграции производства, управления трудовыми ресурсами, финансового менеджмента и управления активами. ERP ориентирована на непрерывную балансировку и оптимизацию ресурсов предприятия посредством специализированного пакета прикладного программного обеспечения, который обеспечивает общую модель данных и процессов для всех сфер деятельности. ERP-система является конкретным программным пакетом, реализующим стратегию ERP.

С задачей выбора пути информатизации сталкивается практически каждое предприятие на определенной фазе своего развития [1-3]. Один из путей такого развития – это внедрение ERP-системы. В ERP-системе, как в центральной информационной системе предприятия, сосредоточено большое количество конфиденциальной информации. Например, финансовая информация, данные о клиентах, кадровые данные. Раскрытие такой информации может принести предприятию значительные убытки. Поэтому проблемы информационной безопасности особенно актуальны для ERP-систем [4].

Задачами информационной безопасности ERP-систем являются:

- уменьшение рисков потери/раскрытия информации;
- соответствие государственным и внутрикорпоративным нормам защиты информации;
- защита целостности данных;
- гарантия конфиденциальности внутренней информации предприятия.

Информационную безопасность необходимо обеспечить для всех компонентов ERP-системы, поэтому рассмотрим ее архитектуру.

Современная ERP-система состоит из трех компонентов, связанных через клиент-серверную архитектуру (рис. 1).

Выделяют следующие уровни ERP-системы:

- уровень базы данных (БД);
- уровень приложений;
- уровень представления (пользовательский).

Трехуровневая клиент-серверная архитектура может расширяться в многоуровневую систему. При этом добавляются компоненты для работы с Интернетом, что в инфраструктуре системы SAP, например, обеспечивается с помощью Internet Transaction Server (ITS).

Хранение данных осуществляется в базе данных (уровень БД), их обработка выполняется на сервере приложений (уровень приложений), а непосредственное взаимодействие с пользователем происходит через клиентскую программу (уровень представления). В качестве такой программы в последнее время используется веб-браузер.

1 Булдакова Татьяна Ивановна, доктор технических наук, профессор, МГТУ им. Н.Э. Баумана, Москва, buldakova@bmstu.ru,
2 Коршунов Алексей Витальевич, МГТУ им. Н.Э. Баумана, Москва, korshun3101@rambler.ru.

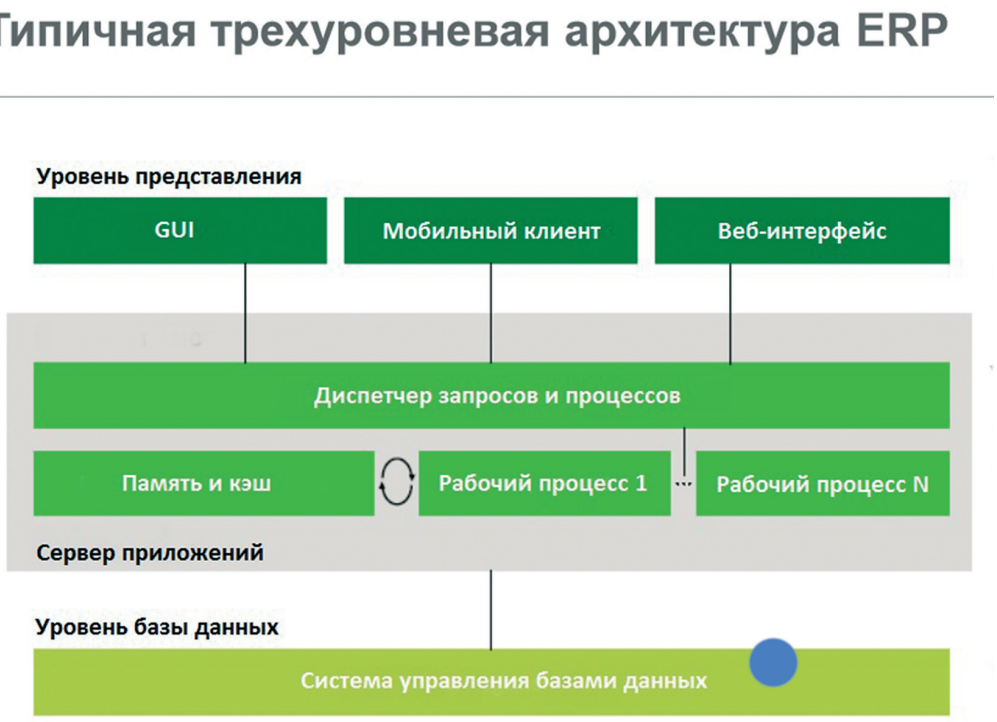

***Рис. 1**. Архитектура ERP-системы*

Обеспечение той или иной степени защищенности информации возможно на каждом из этих уровней. Выбор механизмов защиты информации на вышеуказанных уровнях ERP-системы зависит от специфики конкретного проекта [4].

Связующей средой для компонентов, находящихся на различных архитектурных уровнях ERP, является сетевая инфраструктура. В итоге, можно выделить следующие основные аспекты безопасности:

- сетевая безопасность;
- безопасность БД;
- безопасность на уровне сервера приложений;
- защита информации на клиентском компьютере.

1. Сетевая безопасность ERP

Рассмотрим способы обеспечения информационной безопасности сетевой инфраструктуры. Многие современные ERP-системы, например SAP NetWeaver или Oracle e-Business Suite, применяют веб-стандарты для построения взаимодействия своих компонентов.

В SAP беспарольная аутентификация и шифрование каналов связи реализуются с использованием механизма SNC (Secure Network Communications) при обмене данными по протоколу DIAG и протокола SSL/TLS при обмене данными по HTTP/FTP [5]. Вендор предоставляет средства поддержки SNC для межсерверного взаимодействия, а также, на условиях дополнительного лицензирования, средства ограниченной поддержки SNC для клиентских ПК (SAP NetWeaver Single-Sign-On). При этом пользователям рекомендуется использовать полнофункциональные партнерские решения. Так как правовое положение иностранной криптографии в России неоднозначно, а поставка таких средств может быть ограничена возможными санкциями, целесообразно использовать реализации SNC с «гостированной» криптографией. Кроме того, такие продукты дешевле зарубежных аналогов, и их техническая поддержка существенно ближе к заказчику [6].

В штатную поставку многих ERP-систем не входят российские сертифицированные средства защиты информации, поскольку большая часть таких систем создается зарубежными компаниями SAP, Oracle и другими. Поэтому при внедрении таких ERP-систем необходима установка дополнительного программного обеспечения.

2. Безопасность базы данных ERP

Одним из важнейших компонентов ERP-системы является БД. Базу данных для ERP-системы можно разместить на том же физическом сервере, на котором работает и сервер приложений, но, как правило, для БД выделяются один или несколько отдельных серверов. Целесообразно программно и физически изолировать эти серверы от остальной компьютерной инфраструктуры компании. Рекомендуется строго ограничивать доступ к фи-

зическим серверам и компонентам оборудования. Например, оборудование сервера базы данных и сетевые устройства должны находиться в закрытых охраняемых помещениях. Доступ к резервным носителям также следует ограничить.

Операционная система, под которой работает СУБД ERP-системы, тоже должна быть настроена таким образом, чтобы доступ к БД был открыт только серверу приложений. Ни один пользователь ERP-системы не должен иметь прямого доступа к базе данных [5].

3. Безопасность на уровне сервера приложений

На сервере приложений происходит обработка данных, и тем самым он обеспечивает авторизацию пользователей, то есть запрещает или разрешает доступ к различным объектам ERP-системы [4].

В большинстве современных ERP-систем применяется модель RBAC (Role-Based Access Control, управление доступом на основе ролей) для того, чтобы позволить пользователям выполнять только строго определённые транзакции и получать доступ лишь к определённым бизнес-объектам. В модели RBAC решения о предоставлении доступа пользователю принимаются на основе функций, которые пользователь выполняет в организации [7].

Роль можно понимать как множество транзакций, которые пользователь или группа пользователей могут совершать в организации. Транзакция - это некоторая процедура по преобразованию данных в системе, плюс данные, над которыми эту процедуру можно выполнять [8]. Всякой роли соответствует множество пользователей, которые принадлежат этой роли. У пользователя может быть несколько ролей. Одним из достоинств модели RBAC является удобство администрирования [9].

Назначенная пользователю роль состоит из набора полномочий, и именно наличие необходимого полномочия проверяет сервер во время выполнения транзакции. Таким образом, наличие полномочий позволяет достичь необходимого уровня детализации в разграничении доступа. Следует заметить, что необходимые роли и соответствующие им полномочия должны быть основаны на четко определенной организационной структуре и бизнес-процессах, которые предприятие стремится автоматизировать за счет внедрения ERP-системы. Поэтому данные об организационной структуре должны быть доступны до начала проектирования набора необходимых ролей для пользователей [10-12].

4. Безопасность на уровне представления

Последней линией защиты информации является непосредственно рабочее место пользователя, то есть клиентский компьютер. Статистика говорит, что большинство преступлений в сфере IT совершается самими сотрудниками фирмы, а не внешними злоумышленниками [4].

Первое «узкое» место - это вход пользователя в систему. Традиционный подход предполагает, что у пользователя есть имя и пароль для входа в ОС и другие имя и пароль для входа в ERP-систему. У такого подхода множество недостатков. Альтернативой традиционному подходу может служить аутентификация пользователя с помощью цифровых сертификатов, тем более что те или иные механизмы на основе PKI есть в большинстве современных ERP-систем. Соответственно, можно в числе прочего достичь реализации концепции Single Sign On (единый вход в систему). Концепция Single Sign On подразумевает, что для входа в различные информационные системы пользователь проходит процедуру аутентификации только один раз.

Для защиты устройств ввода/вывода существуют различные дополнительные программные средства, устанавливаемые непосредственно на клиентский компьютер. Для защиты от утечек информации по различным каналам используются специальные системы предотвращения утечек.

Заключение

Подводя итоги, можно сделать следующий основной вывод: сложность ERP-системы ведёт к возникновению ее уязвимостей. ERP-системы обрабатывают большое число различных транзакций и реализуют сложные механизмы, которые предоставляют разные уровни доступа разным пользователям. Практически для любой ERP помимо штатных средств защиты информации, как правило, требуются дополнительные программные средства, в том числе криптографические, и привлечение сторонних поставщиков для выполнения всех требований по информационной безопасности.

Перечисленные выше механизмы обеспечения защиты должны составлять основу системы безопасности ERP. Эти средства обеспечивают защиту на уровне отдельных компонентов ERP-системы. Как правило, системы безопасности влекут за собой высокую стоимость проекта и низкую производительность. Такие противоречия всегда существуют. Необходимо соблюдать баланс между безопасностью, производительностью и удобством использования ERP.

Рецензент: Матвеев Валерий Александрович, доктор технических наук, профессор, v.a.matveev@bmstu.ru

Литература:

1. Булдакова Т.И., Карагод А.Л., Суятинов С.И. Пути информатизации отечественных предприятий // Перспективы культурно-цивилизационной эволюции общества: межвузовский научный сборник. Саратов: СГТУ, 2003. С. 233-238.
2. Булдакова Т.И., Суятинов С.И. Информационно-аналитическая система управления снабжением и производством инструмента // Информационные технологии. 2002. №11. С. 28-33.
3. Булдакова Т.И., Суятинов С.И. Идентификация и исследование сложных систем. Саратов: СГТУ, 2009. 108 с.
4. Егорова Г.В., Шляпкин А.В. Информационная безопасность ERP-систем // Информационные системы и технологии: управление и безопасность. 2013. №2. С. 202-211.
5. Кале В. Внедрение SAP R/3. Руководство для менеджеров и инженеров. М: Компания АйТи, 2004. 511 с.
6. Ненашев С.А. Криптографическая защита информации в ERP-системах компании SAP // Information Security/ Информационная безопасность. 2009. №3. С. 24-25.
7. Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: ДМК Пресс, 2006. 400 с.
8. Дэниел О'Лири. ERP-системы: выбор, внедрение, эксплуатация. Современное планирование и управление ресурсами предприятия. М.: Вершина, 2004. 272 с.
9. Eyers D.M., Bacon J., Moody K. Oasis role-based access control for electronic health records // IEEE Software. 2006. Pp. 16-23.
10. Булдакова Т.И., Миков Д.А. Анализ информационных процессов виртуального центра охраны здоровья // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2014. № 2. С. 10-20.
11. Sandhu R., Coyne E.J., Feinstein H.L., Youman C.E. Role-Based Access Control Models. // IEEE Computer. 1996. 29 (2). Pp. 38–47.
12. Feltus C., Petit M., Sloman M. Enhancement of Business IT Alignment by Including Responsibility Components in RBAC // Proceedings of the CAiSE. Workshop Business/IT Alignment and Interoperability (BUSITAL2010). 2010. Vol. 599. Pp. 61-75.

INFORMATION SECURITY OF ERP-SYSTEMS

Buldakova T.I.[3], Korshunov A.V.[4]

This article shows the basic mechanisms of information security ERP–systems. These systems represent a software package for managing, balancing and optimizing enterprise resources, they provide a common data model and processes for all areas of the company. The main aspects of security ERP–systems are shown. Now to ensure information security in the ERP–system in addition to full–time information security tools the additional software, including cryptography, are used to fulfill all the requirements for information security. This article provides a structured view of all the mechanisms of information security management systems. We consider network security of ERP–systems, and also security at the database level, the application server level and level representation. It is discussed the question of providing access to the user based on the model of RBAC.

Keywords*: ERP–system, network security of ERP–systems, application server, presentation layer, model RBAC*

References:

1. Buldakova T.I., Karagod A.L., Suyatinov S.I. Puti informatizatsii otechestvennyih predpriyatiy, Perspektivyi kulturno-tsivilizatsionnoy evolyutsii obschestva: mezhvuzovskiy nauchnyiy sbornik. Saratov: SGTU, 2003, pp. 233-238.
2. Buldakova T.I., Suyatinov S.I. Informatsionno-analiticheskaya sistema upravleniya snabzheniem i proizvodstvom instrumenta, Informatsionnyie tehnologii. 2002. No 11, pp. 28-33.
3. Buldakova T.I., Suyatinov S.I. Identifikatsiya i issledovanie slozhnyih sistem. Saratov: SGTU, 2009. 108 p.
4. Egorova G.V., Shlyapkin A.V. Informatsionnaya bezopasnost ERP-sistem, Informatsionnyie sistemyi i tehnologii: upravlenie i bezopasnost. 2013. No 2, pp. 202-211.
5. Kale V. Vnedrenie SAP R/3. Rukovodstvo dlya menedzherov i inzhenerov. M: Kompaniya AyTi, 2004. 511 p.
6. Nenashev S.A. Kriptograficheskaya zaschita informatsii v ERP-sistemah kompanii SAP, Informatsionnaya bezopasnost [Information Security]. 2009. No 3, pp. 24-25.
7. Petrenko S. A., Kurbatov V. A. Politiki informatsionnoy bezopasnosti. M.: DMK Press, 2006. 400 p.
8. Deniel O'Liri. ERP-sistemyi: vyibor, vnedrenie, ekspluatatsiya. Sovremennoe planirovanie i upravlenie resursami predpriyatiya. M.: Vershina, 2004.
9. Eyers D.M., Bacon J., Moody K. Oasis role-based access control for electronic health records, IEEE Software. 2006, pp. 16-23.
10. Buldakova T.I., Mikov D.A. Analiz informatsionnykh protsessov virtual'nogo tsentra okhrany zdorov'ya, Nautchno-tekhnitcheskaya informatsiya. Seriya 2: Informatsionnye protsessy i sistemy. 2014. No 2, pp. 10-20.
11. Sandhu R., Coyne E.J., Feinstein H.L., Youman C.E. Role-Based Access Control Models, IEEE Computer. 1996. 29 (2), pp. 38–47.
12. Feltus C., Petit M., Sloman M. Enhancement of Business IT Alignment by Including Responsibility Components in RBAC, Proceedings of the CAiSE. Workshop Business/IT Alignment and Interoperability (BUSITAL2010). 2010. Vol. 599, pp. 61-75.

3 Tatyana Buldakova, Doctor of Technical Sciences, Professor, Bauman Moscow State Technical University, Moscow, buldakova@bmstu.ru.

4 Aleksey Korshunov, Bauman Moscow State Technical University, Moscow, korshun3101@rambler.ru.