DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.3.4
УДК 004.056
ББК 32.972.1

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ERP-СИСТЕМ

Григорий Владимирович Жарков

Студент,
Волгоградский государственный университет
g89954113431@yandex.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Сергей Васильевич Пшеничный

Ассистент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Марина Ивановна Ожиганова

Кандидат технических наук,
доцент кафедры информационной безопасности,
Севастопольский государственный университет
vip.tapki@list.ru
ул. Курчатова, 7, 299015 г. Севастополь, Российская Федерация

Аннотация. В данной статье описана основная структура ERP-систем. Приведена статистика распространенности ERP-систем на мировом рынке. Рассмотрены разнообразныеспособы защиты для основных уровней ERP-системы. Проанализированы как общие, так и индивидуальные методы защиты данных ERP-системы.

Ключевые слова: методы защиты, защищенность, ERP-система, безопасность, риск.

© Жарков Г.В., Пшеничный С.В., Ожиганова М.И., 2018

Введение

ERP (англ. Enterprise Resource Planning «планирование ресурсов предприятия») – организационная стратегия интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами, ориентированная на непрерывную балансировку и оптимизацию ресурсов предприятия посредством специализированного интегрированного пакета прикладного программного обеспечения, обеспечивающего общую модель данных и процессов для всех сфер деятельности. ERP-система является конкретным программным пакетом, реализующим стратегию ERP [6].

Сегодня многие современные компании используют ERP-системы как эффективное средство автоматизации и ускорения процессов ведения бизнеса. Большинство ERP-систем обладают внушительным функционалом, таким как ведение конструкторских и технологических спецификаций, управление спросом и формирование планов продаж и производства, планирование потребностей в мате-

риалах, управление запасами и закупочной деятельностью, планирование производственных мощностей, финансовые функции, функции управления проектами [4]. Однако в связи с тем, что ERP-система объединяет практически все информационные процессы предприятия и осуществляет хранение, обработку и передачу данных, возрастает и риск информационных угроз, что, в свою очередь, влечет за собой большие убытки для компании.

На данный момент большинство ERP-систем имеют трехзвенную клиент-серверную архитектуру (см. рис. 1), а именно:

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

Вся информация компании структурирована и хранится в базе данных (уровень БД), анализ данных происходит на сервере приложений (уровень приложений), а взаимодействие с пользователем – через программу с понятным графическим интерфейсом (уровень представления). В роли такой клиентской программы часто используют веб-браузер. Связующей средой для передачи информации между различными уровнями архитектуры ERP является сетевая инфраструктура.

Panorama Consulting Solutions опубликовала итоги ежегодного исследования общемирового рынка ERP 2018 [2] (см. рис. 2). В опросе приняли участие 200 представителей крупного, среднего и малого бизнеса. 91 % респондентов – из Северной Америки, 7 % –

Рис. 1. Архитектура ERP-системы

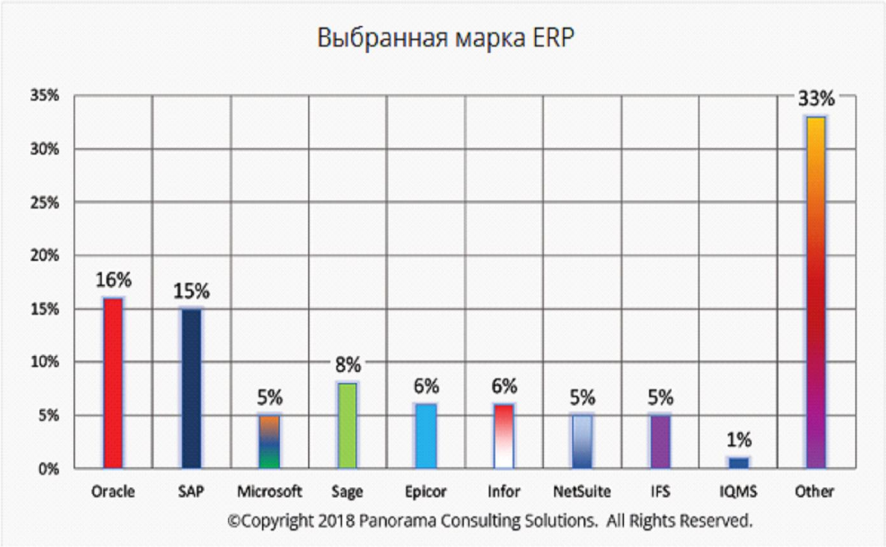

Рис. 2. Мировой рынок ERP-систем

из Европы, 2 % – из Азии. В результате этого исследования выяснилось, что американские и европейские заказчики выбирают ERP-решения таких производителей, как Oracle, SAP и Sage. При этом 42 % заказчиков отдают предпочтение системам минимального уровня надежности Tier I. Такие системы, как правило, содержат широкий набор функций и зачастую стоят дороже. Поставщики решений уровня Tier II предлагают пакеты ПО средней сложности.

Проанализировав структуру ERP-системы, можно выделить следующие методы защиты:

1. Защита сетевой инфраструктуры.

Одним из способов обеспечения защиты сети является использование протоколов с шифрованием данных, таких как:

1) HTTPS – работает через шифрованные транспортные механизмы SSL и TSL. Он обеспечивает защиту от атак, основанных на прослушивании сетевого соединения – от снифферских атак и атак типа man-in-the-middle [7].

2) WEP – первый протокол безопасности, описанный стандартом IEEE 802.11. Для шифрования данных он использует ключ длиной 40–104 бит. Кроме того, дополнительно применяется шифрование, основанное на алгоритме RC4, который называется алгоритмом обеспечения целостности данных [8].

Кроме того, совместно с защищенными протоколами возможно использование механизмов аутентификации. Примером такого комбинирования является использование технологии SNC в ERP-системе SAP.

2. Защита базы данных.

Защита базы данных является одним из самых важных аспектов информационной безопасности предприятия. Первой линией защиты служат физическое изолирование сервера БД от других компонентов ERP-системы и настройка межсетевых экранов перед СУБД, чтобы заблокировать любые попытки доступа от сомнительных источников. Также следует обеспечить контроль аудита действий пользователя.

3. Защита сервера приложений.

С ростом предприятия увеличивается и количество сотрудников, которые должны выполнять строго определенные функции. И в связи с этим возникает проблема ограничения доступа сотрудников к проектам, не связанным с их деятельностью, поэтому главным методом защиты сервера приложений является использование наиболее надежных технологий по разграничению функционала сотрудников. В большинстве ERP-систем применяют технологию RBAC, которая основана на распределении ролей. Такого рода разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы правила разграничения [5]. Однако бизнес-правила неизбежно усложняются и становятся многомерными, и из этого следует, что одной роли для выражения бизнес-процессов становится недостаточно. Чтобы справиться с этой сложностью, приходится создавать дополнительные роли. Это решение означает усложнение системы ролей и может повлиять на безопасность системы. Выходом из ситуации стала технология ABAC. Основное отличие этого подхода заключается в том, что каждая ситуация оценивается не с точки зрения роли пользователя и действия, которое он хочет совершить, а с точки зрения атрибутов, которые к ним относятся. Бизнес-правило, по сути, представляет собой набор условий, в которых различные атрибуты должны удовлетворять предъявляемым к ним требованиям [3].

4. Защита клиентского компьютера.

Первой проблемой защиты данного компонента является аутентификация сотрудников. Традиционный подход предполагает, что у пользователя есть логин и пароль для входа в ОС и другой логин и пароль для входа в ERP-систему. Это, в свою очередь, означает, что возрастает риск кражи пользовательских данных. Решением данной проблемы является аутентификация пользователя с помощью цифровых сертификатов. Статистика говорит, что большинство IT-преступлений совершается самими сотрудниками фирмы, а не внешними злоумышленниками [1]. Поэтому для обеспечения безопасности клиентского компьютера необходима установка дополнительных программ, обеспечивающих контроль передачи и хранения информации. Следовательно, необходимо задуматься об установке антивирусных программ для выявления вредоносного ПО.

На основании вышеизложенного можно сделать вывод, что сложность ERP-системы увеличивает риск информационных утечек. Для обеспечения информационной безопасности ERP-системы необходимо применять большое количество методов и средств защиты, что, в свою очередь, означает увеличение затрат и снижение производительности предприятия. Поэтому одной из основных задач компании любого уровня является соблюдение баланса между безопасностью и производительностью.

СПИСОК ЛИТЕРАТУРЫ

1. Егорова, Г. В. Информационная безопасность ERP-систем / Г. В. Егорова, А. В. Шляпкин // Информационные системы и технологии: управление и безопасность. – 2013. – № 2. – С. 202–211.

2. Обзор мирового рынка ERP 2018. – Электрон. текстовые дан. – Режим доступа: http://www.sfx-tula.ru/news/infoblog/9158/ (дата обращения: 11.10.2018). – Загл. с экрана.

3. Подходы к контролю доступа: RBAC vs. ABAC. – Электрон. текстовые дан. – Режим доступа: https://habr.com/company/custis/blog/248649/ (дата обращения: 10.10.2018). – Загл. с экрана.

4. Проблемы информационной безопасности при использовании ERP-систем / В. С. Оладько, А. А. Белозерова, С. Ю. Микова, М. А. Нестеренко // Молодой ученый. – 2016. – № 12. – С. 346–348.

5. Управление доступом на основе ролей. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC_%D0%BD%D0%B0_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B5_%D1%80%D0%BE%D0%BB%D0%B5%D0%B9 (дата обращения: 08.10.2018). – Загл. с экрана.

6. ERP. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki/ERP (дата обращения: 03.10.2018). – Загл. с экрана.

7. HTTPS. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki/HTTPS (дата обращения: 05.10.2018). – Загл. с экрана.

8. WEP. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki/WEP (дата обращения: 07.10.2018). – Загл. с экрана.

REFERENCES

1. Egorova G.V., Shlyapkin A.V. Informatsionnaya bezopasnost ERP-sistem [Information Security of ERP-Systems]. *Informatsionnye sistemy i tekhnologii: upravlenie i bezopasnost*, 2013, no. 2, pp. 202-211.

2. *Obzor mirovogo rynka ERP 2018* [Overview of the Global ERP Market 2018]. URL: http://www.sfx-tula.ru/news/infoblog/9158/ (accessed 11 October 2018).

3. *Podkhody k kontrolyu dostupa: RBAC vs. ABAC* [Approaches to Access Control: RBAC vs. ABAC]. URL: https://habr.com/company/custis/blog/248649/ (accessed 10 October 2018).

4. Oladko V.S., Belozerova A.A., Mikova S.Yu., Nesterenko M.A. Problemy informatsionnoy bezopasnosti pri ispolzovanii ERP-sistemy [Problems of Information Security When Using ERP-Systems]. *Molodoy uchenyy*, 2016, no. 12, pp. 346-348.

5. *Upravlenie dostupom na osnove roley* [Role-Based Access Control]. URL: https://ru.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8 %D0%B5_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC_%D0%BD%D0%B0_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B5_%D1%80%D0%BE%D0%BB%D0%B5%D0%B9 (accessed 8 October 2018).

6. *ERP*. URL: https://ru.wikipedia.org/wiki/ERP (accessed 3 October 2018).

7. *HTTPS*. URL: https://ru.wikipedia.org/wiki/HTTPS (accessed 5 October 2018).

8. *WEP*. URL: https://ru.wikipedia.org/wiki/WEP (accessed 7 October 2018).

ANALYSIS OF ERP-SYSTEMS PROTECTION METHODS

Grigoriy V. Zharkov

Student,
Volgograd State University
g89954113431@yandex.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Sergey V. Pshenichnyy

Assistant, Department of Information Security,
Volgograd State Uinversity
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Marina I. Ozhiganova

Candidate of Sciences (Engineering),
Associate Professor of Department of Information Security,
Sevastopol State University
vip.tapki@list.ru
Kurchatova St., 7, 299015 Sevastopol, Russian Federation

Abstract. The ERP is an organizational strategy of integration of production and operations, human resources management, financial management and asset management, focused on continuous balancing and optimization of enterprise resources through a specialized integrated software application package that provides a common model of data and processes for all areas of activity. An ERP system is a specific software package that implements the ERP strategy.

Today, many modern companies use ERP-systems as an effective means of automation and acceleration of business processes. Most ERP-systems have impressive functionality such as maintenance of design and technological specifications, demand management and formation of sales and production plans, material requirements planning, inventory and procurement management, production capacity planning, financial functions, project management functions. However, due to the fact that the ERP-system combines almost all information processes of the enterprise and carries out storage, processing and transmission of data, the risk of information threats increases, which in turn entails large losses for the company. After analyzing the structure of the ERP-system, the following protection methods can be identified: protection of network infrastructure; database protection; application server protection. Based on the above, we can conclude that the complexity of the ERP-system increases the risk of information leaks. To ensure the information security of the ERP system, it is necessary to apply a large number of methods and means of protection, which in turn means an increase in costs and a decrease in the productivity of the enterprise. Therefore, one of the main tasks of the company at any level is to maintain a balance between safety and performance.

Key words: protection methods, safety, ERP-system, security, risk.