УДК 004.6

СПОСОБИ ЗАХИСТУ ERP-СИСТЕМ

Анастасія Сениш, Орест Полотай

кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

В даній роботі виділені основні проблеми, які виникають в плані безпеки інформації при запровадженні покращеної системи корпоративної управління підприємством. Описано особливості ERP-систем, як способу інформатизація корпоративного управління за рахунок впровадження інформаційних технологій.

***Ключові слова**: управління, класи, зовнішні порушники, внутрішні порушники, IT-інфраструктура, компоненти, клієнт-серверна архітектура, основні аспекти безпеки.*

This paper highlights the main problems that arise in terms of information security in the implementation of an improved system of corporate governance. Features of ERP-systems as a way of informatization of corporate management due to introduction of information technologies are described.

***Key words:** management, classes, external violators, internal violators, IT infrastructure, components, client-server architecture, basic security aspects.*

В даний час вдосконалення корпоративного управління стає ключовим стратегічним завданням розвитку і життєдіяльності будь-якого підприємства. В силу того, що практично всі способи вдосконалення управління вичерпані, єдиним способом виживання в конкурентній боротьбі залишаються інтенсивні способи поліпшення управління.

Одним з таких способів є інформатизація корпоративного управління за рахунок впровадження інформаційних технологій, в тому числі систем класу ERP. Зростання систем обробки, зберігання інформації, а також величезна кількість впроваджуваних нових технологій з якими доводиться стикатися при забезпеченні інформаційної безпеки породжує велику кількість проблем. У зв'язку з цим важливу роль починає відігравати інформаційна безпека, оскільки вся інформація компанії знаходиться в цифровому вигляді. Тому життєво важливо захищати інформацію компанії як від зовнішніх, так і від внутрішніх порушників.

Основну роль в IT-інфраструктурі компанії відіграє ERP-система, яка практично допомагає керувати всіма бізнес процесами компанії, оскільки містить саму важливу бізнес інформацію. Головним механізмом захисту є розмежування повноваження користувачів в ERP-системі. Даний механізм дозволяє відповідно до бізнес ролей кожного співробітника дати йому повноваження по роботі з тією чи іншою інформацією. Це необхідно, оскільки на ринку величезна кількість конкурентів і від того, як працює фірма, як налаштовані її ролі в системі буде залежати її конкурентоспроможність.

Інформаційну безпеку необхідно забезпечити для всіх компонентів ERP-системи, тому розглянемо її архітектуру. Сучасна ERP-система складається з трьох компонентів, пов'язаних через клієнт-серверну архітектури. Виділяють такі рівні ERP-системи:

- рівень бази даних (БД);
- рівень додатків;
- рівень представлення (призначений для користувача).

Забезпечення в тій чи іншій мірі захищеності інформації можливо на кожному з цих рівнів. Вибір механізмів захисту інформації на вищевказаних рівнях ERP-системи залежить від специфіки конкретного проекту. Сполучним середовищем для компонентів, що знаходяться на різних архітектурних рівнях ERP, є мережева інфраструктура.

У підсумку, можна виділити наступні основні аспекти безпеки:

- мережева безпека;

- безпека БД;
- безпека на рівні сервера додатків;
- захист інформації на клієнтському комп'ютері.

ERP-системи обробляють велику кількість різних транзакцій і реалізують складні механізми, які надають різні рівні доступу різним користувачам.

Для забезпечення надійного захисту ERP-системи на сьогодні і в подальшому, у системі інформаційної безпеки повинні бути реалізовані найпрогресивніші технології. Основними положеннями щодо безпеки є:

- аналіз і дослідження причин порушення інформаційної безпеки;
- розробка результативних моделей безпеки які будуть відповідати сучасному розвитку апаратних і програмних засобів;
- створення методів і засобів коректного впровадження моделей безпеки в існуючі обчислювальні системи, з можливістю гнучкого управління, безпекою в залежності від висунутих вимог, допустимого ризику та витрати ресурсів;
- необхідність розробки засобів аналізу безпеки комп'ютерних систем за допомогою здійснення тестових впливів (атак).

Ролі та обов'язки персоналу щодо захисту інформації є ключем до успіху в будь-якій програмі забезпечення безпеки. Чітке визначення цих ролей і обов'язків необхідно і повинно бути закріплено на етапі впровадження ERP-системи.

Практично для будь-якої ERP, крім штатних засобів захисту інформації, як правило, потрібні додаткові програмні засоби, в тому числі криптографічні, і залучення сторонніх постачальників для виконання всіх вимог з інформаційної безпеки. Саме тому дослідження можливих рішень захисту ERP-системи на сьогоднішній день є актуальним питанням.

Література:

1. О'Лири Д. ERP-системы. Современное планирование и управление ресурсами предприятия. Выбор, внедрение, эксплуатация. М.: Вершина, 2014. 272с.
2. Егорова Г.В., Шляпкин А.В. Информационная безопасность ERP-систем// Информационные системы и технологии: управление и безопасность. 2013. №2. С.202-211.
3. https://uk.wikipedia.org/wiki/Планування_ресурсів_підприємства
4. Д. В. Катрич, В. М. Бурлаков Захист інформації в ERP-системі підприємства // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління» № 2' (31) 2017