УДК. 004.6

Д. В. Катрич, В. М. Бурлаков

ЗАХИСТ ІНФОРМАЦІЇ В ERP-СИСТЕМІ ПІДПРИЄМСТВА

Анотація: У статті досліджено основні механізми забезпечення інформаційної безпеки ERP-систем. Дані системи являють собою сукупність програм, призначених для управління, балансування і оптимізації ресурсів підприємства, вони забезпечують загальну модель даних і процесів для всіх сфер діяльності підприємства. Розглянуто основні аспекти безпеки при роботі з системами, що реалізовують ERP-стратегію. В даний час для забезпечення інформаційної безпеки в ERP-системах, крім штатних засобів захисту інформації, використовуються додаткові програмні засоби, в тому числі криптографічні, щоб виконати всі вимоги з інформаційної безпеки. Дана стаття дає структуроване уявлення про всі механізми забезпечення інформаційної безпеки в системах управління підприємством. Розглянуто мережеву безпеку ERP-систем, а також безпеку на рівні бази даних, рівні сервера додатків і рівні представлення який призначений для користувачів.

Ключові слова: ERP-система, комплексна система захисту інформації, мережева безпека ERP-систем, інформаційна безпека.

Опис проблеми

Інформаційна інфраструктура компанії являє собою великий і складний комплекс, важливою складовою якого є інтегрована система управління інформаційними ресурсами підприємства (ERP-система). Така система потрібна для об'єднання даних і процесів організації, таких як облік основних засобів, кадровий облік, взаємодія з клієнтами, логістика та фінанси, в єдину систему. В ідеалі ERP-система автоматизує всі можливі сфери діяльності підприємства, прискорює і спрощує роботу персоналу, дає в руки менеджменту потужний інструмент для аналізу ефективності і планування.

Із завданням вибору шляху інформатизації стикається практично кожне підприємство на певній фазі свого розвитку. Один із шляхів такого розвитку - це впровадження ERP-системи. В ERP-системі, як в центральній інформаційній системі підприємства, зосереджена велика кількість конфіденційної інформації. Наприклад, фінансова інформація, дані про клієнтів, кадрові дані. Саме тому кожна ланка ERP-системи має бути надійно захищена, так як негативний зовнішній або внутрішній вплив на будь-яку її ділянку може мати найсерйозніші наслідки для діяльності всієї організації. Розкриття такої інформації може принести підприємству значних збитків. Тому проблема інформаційної безпеки особливо актуальна для ERP-систем.

Аналіз останніх досліджень та публікацій

Загальні вимоги, які необхідні для створення інформаційної безпеки в інформаційно-телекомунікаційних системах регламентовані в [3 - 6]. В [7] викладені основні концептуальні питання щодо інформаційної безпеки і загальні питання технічного захисту інформації в інформаційних системах. На сьогодні, нажаль, приділяється недостатньо уваги побудові комплексної системи захисту ERP-системи.

Метою статті є розгляд основних механізмів забезпечення інформаційної безпеки ERP-систем.

Виклад основного матеріалу

Розмірковуючи про інформаційну безпеку в ERP, можна почати з визначення цілей, яких ми хочемо досягти в своїй системі. Отже, головні цілі і завдання інформаційної безпеки це:

- зменшення ризиків втрати / розкриття інформації;
- відповідність державним і внутрішньокорпоративним нормам захисту інформації;
- захист цілісності даних;
- гарантія конфіденційності внутрішньої інформації підприємства.

Розглянемо як і якими засобами можна вирішувати перераховані завдання. Почнемо з розгляду архітектури типової ERP-системи. Сучасна ERP-система має триланкову клієнт-серверну архітектуру, це: рівень бази даних (БД), рівень додатків і рівень представлення (призначений для користувача) [1] (рис. 1).

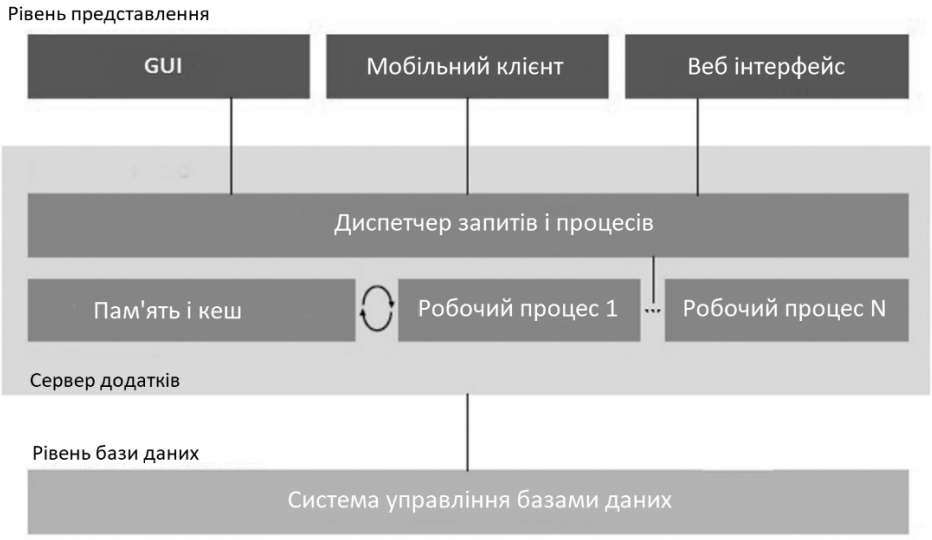

Рис. 1. – Архітектура ERP-системи

Зберігання даних здійснюється в базі даних (рівень БД), їх обробка - на сервері додатків (рівень додатків) і безпосередня взаємодія з користувачем відбувається через програму "Клієнт" з графічним інтерфейсом (рівень представлення).

 ISSN 1560-8956

У ролі такої клієнтської програми останнім часом часто використовується веб-браузер.

Забезпечення в тій чи іншій мірі захищеності інформації можливо на кожному з цих рівнів. Зв’язуючим середовищем для компонентів, що знаходяться на різних архітектурних рівнях ERP, є мережева інфраструктура. У підсумку, розмірковуючи про інформаційну безпеку, умовно можна виділити наступні основні аспекти:

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

Такі рівні в сукупності власне і складають ERP як систему. Розгляне кожен з цих рівнів.

Мережева безпека

Почнемо з розгляду способів забезпечення інформаційної безпеки мережевої інфраструктури. Багато сучасних ERP-систем, наприклад SAP NetWeaver або Oracle e-Business Suite, застосовують веб-стандарти для побудови взаємодії своїх компонентів. В цьому випадку для захисту трафіку можна використовувати протокол HTTPS. Додатково до шифрування трафіку HTTPS також може забезпечувати автентифікацію користувача на основі цифрових сертифікатів.

SAP NetWeaver та Oracle e-Business Suite дозволяють прив'язувати сертифікат до облікового запису користувача ERP-системи. Таким чином, автентифікація користувачів в ERP може бути побудована на основі вже наявної на підприємстві інфраструктури PKI. Інфраструктура PKI(Public Key Infrastructure) призначена для надійного функціонування корпоративних інформаційних систем дозволяє як внутрішнім, так і зовнішнім користувачам безпечно обмінюватися інформацією [9, с. 172]. Коли мова заходить про криптографії, відразу постає питання про те, які саме криптографічні алгоритми слід використовувати. Для багатьох підприємств це питання вирішується однозначно - відповідно з юридичними вимогами необхідно застосовувати криптоалгоритми ДСТУ і, отже, українські сертифіковані криптографічні засоби захисту [2].

Для використання HTTPS на основі західних криптоалгоритмів (DES, RSA і т.д.), як правило, досить вбудованих засобів операційної системи. Так, в MS Windows вже є вбудована підтримка HTTPS на основі DES, RSA і інших західних алгоритмів. З українською криптографією складніше. Не дивно, що в штатну поставку багатьох ERP-систем не входить українські сертифіковані засоби захисту інформації, оскільки велика частина таких систем створюється зарубіжними компаніями - SAP, Oracle та іншими.

Якщо в ERP-системах зарубіжного виробництва потрібно українська криптографія, то необхідно додаткове програмне забезпечення. На вітчизняному ринку представлено кілька подібних рішень.

На платформі SAP NetWeaver крім HTTPS для захисту трафіку і автентифікації користувачів також може бути передбачений протокол Secure Network Communication SNC. Одне з рішень, яке представлено на українському ринку це “UALib”, в ньому правильно реалізовані криптографічні алгоритми, відповідно до вимог ГОСТ 34.311-95, ДСТУ 4145-2002, ДСТУ ГОСТ 28147:2009 [2].

Безпека БД

Припустимо, мережа у нас надійно захищена, тепер необхідно розібратися з джерелами даних, які по цій мережі передаються. Одним з найважливіших компонентів ERP-системи можна вважати базу даних. Як її захистити? БД для ERP-системи можна розмістити на тому ж фізичному сервері, на якому працює і сервер додатків, але, як правило, для БД виділяють один або кілька окремих серверів. Доцільно програмно і фізично ізолювати ці сервери від решти комп'ютерної інфраструктури компанії. Для мережевої ізоляції слід виділити всі сервери БД в один ізольований сегмент локальної корпоративної мережі і надати доступ до цього сегменту тільки серверам додатків [8, ст.724]. Таким чином, виключається можливість доступу по мережі безпосередньо до БД системи.

Операційна система, під якою працює СУБД нашої ERP-системи, теж повинна бути налаштована таким чином, щоб доступ до БД був відкритий тільки серверу додатків. Жоден користувач ERP не повинен мати прямого доступу до бази даних. Важливо подбати і про фізичний захист серверів БД - слід помістити ці комп'ютери в окреме приміщення з контролем доступу.

Безпека на рівні сервера додатків

"Серце" ERP-системи - це сервер додатків. Саме на ньому відбувається обробка даних, і саме сервер додатків забезпечує авторизацію користувачів, тобто забороняє або дозволяє доступ до різних інформаційних об'єктів ERP-системи. Розглянемо концепцію авторизації користувачів на прикладі системи SAP R/3 (зауважимо, що підсистема авторизації не зазнала істотних змін і в SAP NetWeaver). Для кожного користувача SAP R/3 в системі зберігається свій обліковий запис. Цей запис, крім ідентифікатора і пароля, персональних даних та іншої додаткової інформації, зберігає ролі, присвоєні даному користувачеві. На основі призначених користувачеві ролей, сервер додатків дає доступ на виконання різних програм (транзакцій в термінах SAP R/3) [10]. Але деталізація авторизації не обмежується доступом до одних транзакцій і забороною доступу до інших. Адже в рамках однієї і тієї ж транзакції можна отримувати доступ до різних даних. Наприклад, користувач може мати доступ до бухгалтерської звітності

свого відділу, але не чужого, хоча доступ до цих даних відбувається через одну і ту ж транзакцію.

Призначена користувачеві роль складається з набору повноважень, і саме наявність необхідного повноваження перевіряє сервер під час виконання транзакції. Таким чином, наявність повноважень дозволяє досягти необхідного рівня деталізації в розмежуванні доступу. Слід зауважити, що необхідні ролі і відповідні їм повноваження повинні бути засновані на чітко визначеній організаційній структурі і бізнес-процесах, які підприємство прагне автоматизувати за рахунок впровадження ERP-системи. Тому дані про організаційну структуру повинні бути доступні до початку проектування набору необхідних ролей для користувачів.

Захист інформації на клієнтському комп’ютері

Остання лінія захисту інформації - це особисте робоче місце користувача, тобто клієнтський комп'ютер. Статистика говорить, що більшість злочинів в сфері IT відбувається самими співробітниками фірми, а не зовнішніми зловмисниками [8, ст.77]. Навіщо ломитися через брандмауер, намагатися встановити різні троянські програми, якщо вкрасти інформацію безпосередньо на робочому місці значно простіше?

Розглянемо потенційні канали витоку інформації на робочому комп'ютері користувача ERP. Перш за все, щоб користувач міг хоч щось зробити, необхідно увійти спочатку в операційну систему, а потім і в саму ERP. Далі, якщо наш передбачуваний зловмисник знайшов інформацію, яку він хоче вкрасти, йому необхідно кудись переписати отримані дані. Отже, необхідно подбати про захист пристроїв введення/виводу. Користувач також може передати викрадену інформацію через мережу - наприклад, через електронну пошту. Що можна протиставити всім цим загрозам?

Перше - вхід користувача в систему. Традиційний підхід передбачає, що у користувача є ім'я і пароль для входу в ОС та інші ім'я та пароль для входу в ERP-систему. У такого підходу безліч недоліків:

- можливість підглянути пароль;
- складні паролі користувачі часто записують десь безпосередньо на робочому місці, і знайти такий пароль не складе труднощів для зловмисника;
- користувачеві необхідно пам'ятати як мінімум два різних пароля (для входу в ОС і в ERP).

Альтернативою традиційному підходу може служити автентифікація користувача за допомогою цифрових сертифікатів, тим більше, що ті чи інші механізми на основі PKI є в більшості сучасних ERP-системах. Відповідно, можна в числі іншого досягти реалізації концепції Single Sign On (єдиний вхід в систему). Single Sign On передбачає, що для входу в різні інформаційні системи користувач проходить процедуру автентифікації тільки один раз [9, с. 215].

Окреме питання: де користувачеві зберігати свій закритий ключ до свого сертифікату? Зберігати його на робочому комп'ютері? Але тоді доступ до нього може отримати інша людина, не кажучи вже про те, що в сучасних ERP-системах користувач не прив'язаний до робочого місця і може працювати, використовуючи різні термінали. Доцільно зберігати закритий ключ на окремому пристрої зберігання даних, який користувач буде носити з собою. У ролі таких пристроїв виступають, наприклад, eToken. Якщо для зберігання ключа використовується окремий пристрій - токен, то таку автентифікацію називають двох факторною [9, с. 192].

Наявність двох факторів автентифікації полягає в тому, що, з одного боку, користувачеві необхідно мати при собі свій токен для входу в систему, а, з іншого - йому потрібно знати PIN-код для доступу до закритого ключа на токені. Тобто тепер, навіть якщо зловмисник підглянув пароль користувача, він все одно не увійде в систему без токена. Точно так само якщо зловмисник вкрав токен, то треба ще дізнатися PIN-код. Таким чином, з'являється додатковий фактор захисту.

При вході в ОС користувач пред'являє свій цифровий сертифікат і вводить пароль або PIN-код для доступу до закритого ключа. Потім той же самий сертифікат (або інший, що знаходиться на тому ж електронному ключі) використовується і для входу в ERP-систему, причому повторне введення PIN-коду вже не потрібно.

Застосування рішень на основі PKI дозволяє інтегрувати ідентифікацію користувачів в ERP з іншими інформаційними системами компанії. Зокрема, такий підхід дозволяє уникати дублювання процедур автентифікації. Як приклад подібних рішень, представлених на українському ринку, можна привести продукти компанії Aladdin - eToken SecurLogon для SAP R/3, eToken SecurLogon для Oracle E-Business Suite.

Для захисту пристроїв введення/виведення існують різні додаткові програмні засоби, що встановлюються безпосередньо на клієнтський комп'ютер. До числа таких програмних засобів відноситься, наприклад, "DeviceLock". Ця система дозволяє контролювати доступ користувача до всіх пристроїв введення/виведення інформації - дисководів, принтерів, USB-портів і т. п. Можна обійтися і взагалі без додаткового ПЗ, просто не передбачати встановлення дисководів і подібних пристроїв введення/виведення на клієнтських терміналах. Перераховані вище механізми забезпечення захисту повинні складати основу системи безпеки ERP. Ці засоби забезпечують захист на системному рівні - на рівні окремих компонентів структури ERP. Додатково, з точки зору архітектури, можна і потрібно розглядати такі непрості прикладні проблеми:

- надійність;
- управління системою безпеки;
- аналіз ризиків витоків інформації;
- захист електронних документів.

Прикладна безпека ERP-систем

Ніхто не стане сперечатися, що перш за все ERP-система повинна безперервно працювати і виконувати свої функції. ERP-система повинна працювати в режимі 24 години сім днів на тиждень або як мінімум безперервно протягом робочого часу співробітників. Адже для будь-якого бізнесу такий збій загрожує великим втратам. Потрібно забезпечити високу ступінь надійності такої системи. Оскільки сьогодні жоден виробник ПО або апаратних засобів не може дати стовідсоткової гарантії надійності своїх рішень, слід заздалегідь передбачити процедури відновлення працездатності системи після збоїв. Необхідною частиною проекту впровадження ERP є розробка стратегії резервного копіювання, відновлення після збоїв, гарячої заміни обладнання і т.п. Всі ці процедури повинні бути чітко визначені на момент початку продуктивного використання ERP.

Також необхідно прогнозувати обсяги даних, що з часом будуть накопичуватись в системі, для того, щоб банальний брак місця на диску сервера не став причиною припинення роботи. Так як ERP являють собою складні системи з великою кількістю користувачів, то основою ефективного управління безпекою повинна служити можливість централізовано змінювати параметри політики безпеки. Такими змінами можуть бути:

- створення і видалення користувачів ERP;
- привласнення прав користувачам;
- оновлення ПЗ на клієнтських комп'ютерах і т.п.

Часто ERP будується не як окрема монолітна система з одним сервером додатків, а як розподілений набір окремих систем. У кожній подібній системі існує свій набір користувачів, які часто дублюються. Непогано було б в такому випадку мати засіб централізованого управління користувачами і їх повноваженнями, і в деяких ERP такі засоби є.

Розглянемо, як приклад, систему SAP R/3. У цій ERP-системі передбачений спеціальний механізм Central User Administration (CUA) для централізованого управління користувачами і їх повноваженнями. CUA дозволяє виконувати наступні функції:

- уніфікацію облікових записів;
- призначення прав користувачам;
- ведення локальних і глобальних властивостей в облікових записах.

Останнім часом в ERP, так само як і в багатьох інших комплексних програмних системах, використовуються портальні технології. Портал - це точка доступу до різних неоднорідних інформаційних систем. Портал також може виконувати функції автентифікації користувачів. У цьому випадку автоматично досягається централізація системи управління користувачами.

Визначимо які завдання ми зможемо вирішити за допомогою управління підсистемою безпеки ERP. Перш за все, нам необхідно контролювати дії користувачів,

щоб запобігати навмисному і ненавмисному витоку інформації [8, ст. 36]. Очевидно, що в ERP-системах існують різні засоби контролю і аудиту дій користувачів. Як на основі цих засобів побудувати систему контролю, яка дозволить дізнатися і попередити витік інформації?

Для кожного конкретного проекту впровадження ERP в залежності від поточних внутрішніх і зовнішніх вимог, буде спроектована своя підсистема контролю. Спробуємо виділити загальноприйняті етапи побудови такої системи:

- Визначення цілей контролю і стратегії відстеження ризиків.
- Аналіз ризиків.
- Визначення засобів контролю.
- Знаходження відповідних засобів контролю для кожного з ризиків.
- Моніторинг і аудит роботи системи контролю.

На першому етапі визначається стратегія системи контролю, заснована на внутрішніх і зовнішніх вимогах до інформаційної безпеки. На другому етапі складається набір ризиків, які будуть відслідковуватися. На третьому етапі визначаються всі доступні в даній ERP-системі механізми контролю. Для прикладу в SAP R/3 в якості засобів контролю може використовуватися системний журнал, в який заносяться такі події:

- відкриття/закриття сесії користувачем;
- запит на доступ до захищеного ресурсу;
- створення і знищення об'єкта;
- дії зі зміни правил розмежування доступу.

Існують також засоби вибіркового ознайомлення з цією реєстраційною інформацією. На четвертому етапі для кожного з ідентифікованих раніше ризиків підбирається засіб його відстеження. П'ятий етап - безпосередньо експлуатація розробленої системи контролю.

Висновки

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).

 ISSN 1560-8956

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.

Список використаних джерел

1. SAP ERP Client Server Architecture [Електронний ресурс] – 2014. – Режим доступу до ресурсу: https://www.esds.co.in/blog/sap-erp-client-server-architecture/#sthash.fSpYnQEc.dpbs

2. Перелік засобів КЗІ, які мають експертний висновок за результатами державної експертизи у галузі КЗІ – 2017. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=111853&cat_id=72110&mustWords=+Перелік+засобів+КЗІ%2C+які+мають+експертний+висновок&searchPublishing=1

3. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31, - с.286.

4. Постанова КМ України “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” № 373 від 29 березня 2006 року. [Електрон. ресурс]: - Режим доступу: http://zakon3.rada.gov.ua/laws/show/373-2006-п.

5. НД ТЗІ 3.7-003-05 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”. [Електрон. ресурс]: - Режим доступу:http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835.

6. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”. [Електрон. ресурс]: - Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342.

7. Методика информационной безопасности. / [Уфимцев Ю.С., Буянов В.П., Ерофеев Е.А и др.] – М.: Издательство “Экзамен”, 2004. – 544 с.

8. Шон Харрис CISSP.Руководство для подготовки к экзамену. – М.: изд-во “ McGraw-Hill Osborne Media ”, 2011. – 875 с.

9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях – М.: изд-во “ДМК Пресс”, 2012. – 592 с.

10. SAP R/3 [Електронний ресурс] – 2017. – Режим доступу до ресурсу: http://www.softline.kiev.ua/avtomatizatsiya-biznesa/erp-sistemy/603-sap-r3.html