УДК 004.036

ІНФОРМАЦІЙНИЙ ЗАХИСТ СИСТЕМИ 1С ПІДПРИЄМСТВО

Рудов О.П., Романченко Т.П., Скріпкіна А.С.

INFORMATION PROTECTION SYSTEM 1C: ENTERPRISE

Pudov A., Romanchenko T., Skripkina A.

В статті розглянуті деякі аспекти розмежування доступу користувачів у комп'ютерних системах бухгалтерського обліку, на прикладі «1С:Підприємство», що є необхідним для забезпечення ефективної організації облікового процесу, та надійного захисту комерційної інформації суб'єкту господарювання.

Ключові слова: *захист інформації, інформаційна система, 1С:Підприємство, розмежування доступу.*

Постановка проблеми. У постіндустріальних (інформаційних) суспільствах інформаційні ресурси є основним чинником економічного зростання. Інформація, створена у комп'ютерних інформаційних системах бухгалтерського обліку підприємства (КІСБО), є власністю цього підприємства і згідно із законами України "Про інформацію" [1] та "Про захист інформації в автоматизованих системах" [2], потребує захисту. Підприємство, як власник інформації, самостійно забезпечує її захист, визначаючи режим доступу до інформації. Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

Загрозу для КІСБО можуть становити три групи осіб: фахівці з комп'ютерних інформаційних систем, користувачі і зловмисники. Результатами порушення прав захисту інформації в КІСБО можуть бути: витік інформації, втрата інформації, підробка інформації, блокування інформації, порушення роботи КІСБО. Крім прямих загроз інформаційним ресурсам існують загрози крадіжок користувачами бухгалтерської системи активів підприємства шляхом включення фіктивних операцій в систему, перекручування інформації, знищення файлів з інформацією тощо. Щоб запобігти кризовим ситуаціям КІС БО щодо користувачів бухгалтерської системи застосовують такі заходи: розподіл обов'язків, нагляд, подвійний контроль, застосування затверджених форм носіїв інформації, незалежні перевірки стану активів у підзвітності матеріально відповідальних осіб, перевірки процесу обробки інформації, розмежування доступу користувачів до функцій системи та інформаційних ресурсів.

Аналіз попередніх досліджень. Облікові системи 1С: Підприємство стають об'єктом підвищеної уваги зловмисників, оскільки містять максимум інформації про діяльність організації. У той же час наявною вбудованої захисту недостатньо для протидії багатьом поширеним загрозам:

несанкціоноване копіювання бази даних;

доступ системного адміністратора до конфіденційної інформації;

втрата або крадіжка носіїв інформації;

неправомірні дії зловмисників: фіктивний арешт майна, вилучення системних блоків, серверів;

шахрайство, обман співробітників і багато іншого.

З метою інтеграції та поділу доступу користувачів до інформації при роботі з програмою «1С: Бухгалтерія 8.0-8.2» в мережі персональних комп'ютерів, можливості платформи «1С: Підприємство 8.0-8.2» дозволяють встановити для кожного користувача права на роботу з інформацією, яка обробляється системою. [3,4] Система «1С: Підприємство 8.0-8.2" дозволяє вести список користувачів, яким дозволена робота з системою. Для кожного користувача може бути задане ім'я, що ідентифікує користувача в системі, повне ім'я, використовуване при відображенні довідкової інформації, порядок аутентифікації користувача системою. Список користувачів дозволяє вказати ролі, які будуть доступні користувачеві при роботі з прикладним рішенням «1С: Бухгалтерія 8.0-8.2», одному користувачеві може бути призначений кілька ролей. Систему ролей, існуючу в конкретному прикладному рішенні, визначає розробник. Обмеження доступу до даних можуть бути накладені як на рівні метаданих, так і на рівні записів і полів бази даних.

Мета роботи. Розмежування доступу користувачів у КІСБО необхідне ще й для того, щоб забезпечити ефективну організацію облікового процесу, юридичну доказовість складених електронних носіїв інформації тощо. Інформаційна система "1С: Підприємство. Версія 8.0-8.2" (Далі - "1С: Підприємство") передбачає систему заходів для забезпечення розмежування доступу користувачів до інформаційної бази програми. Проте, недостатність методичного забезпечення розмежування доступу користувачів спричинює невикористання підприємствами

наданих їм можливостей. Тому ми поставили собі за мету при написанні цієї статті сформувати методику розмежування доступу користувачів у ІС «1С: Підприємство» на прикладі окремого підприємства, використовуючи типову конфігурацію системи "Бухгалтерський облік для України".

Основний матеріал статті. Розглянемо деякі аспекти злому і захисту «1С: Підприємство» в локальній і мережевій версії.

Злом зазвичай складається з 2-х стадій. Перша стадія це викрадання бази методом копіювання, друга стадія це аналіз викраденої бази. Для копіювання бази користувач зазвичай використовує штатні засоби Windows, за допомогою яких копіює на зовнішній носій DBF-файли бази. Аналіз викраденої бази зазвичай проводиться за допомогою MS Excel. Даному методу злому неможливо протидіяти використовуючи програмні рішення на мові 1С. Викрадачеві не потрібно зламувати паролі і обходити програму, він дістає доступ до даних відразу мимо 1С.

Перейдемо тепер до захисту. Розглянемо варіант, коли база даних 1С не зашифрована, зберігається у відомому форматі, закрити доступ користувачів до неї не можна, оскільки вони з нею працюють. Можна спробувати накласти на файли бази атрибут hidden, але самі розумієте це «захист тільки від дурня». Можна ввести жорсткі правила роботи і вилучити дисководи у користувачів. Проте користувачі можуть відправити викрадену базу поштою, проаналізувати її на місці без винесення з офісу. Тобто, надійно захистити базу навіть від недосвідчених користувачів в такому варіанті фактично неможливо.

Зараз на багатьох підприємствах в якості СУБД використовується Microsoft SQL Server. Проте стандартне «1С:Підприємство» не використовує засобу розмежування доступу MS SQL і кожен користувач працює з базою з повними правами (Database Owner, DBO). Логін і пароль DBO простий користувач не знає, він зберігається в зашифрованому вигляді у файлі 1cv8.1cf, див. рис. 1.

Подібний підхід 1С до організації безпеки на MS SQL здається небезпечним. Багато конкурентів 1С програми, що проводять, під MS SQL заявляють як свою конкурентну перевагу, то що авторизація користувачів в їх застосуванні робиться засобами самого MS SQL. Тонкість полягає в тому, що для ефективної організації захисту засобами MS SQL потрібно виключити доступ користувачів до таблиць бази, а вирішити тільки маніпуляції через так звані уявлення (view) і процедури, що зберігаються (stored procedure). Хоча частенько заявляється, що це все є, а реально цього немає, програмісти не встигають робити нові функції, куди ним до захисту даних.

Проблема захисту 1С для MS SQL, точніше загальна проблема захисту класу Application Security Role, полягає в тому, що навіть теоретично не забезпечити надійне шифрування логіна і пароля DBO. Будь-який криптостійкий захист базується на тому, що програма не містить в собі всієї інформації необхідною для розшифровки даних. Зазвичай відсутні дані - це пароль користувача.

Якщо зловмисник знає пароль хоч одного користувача 1С, при будь-якому криптозахисті він зможе розшифрувати пароль DBO, оскільки володіє 100% початковій інформації для розшифровки.

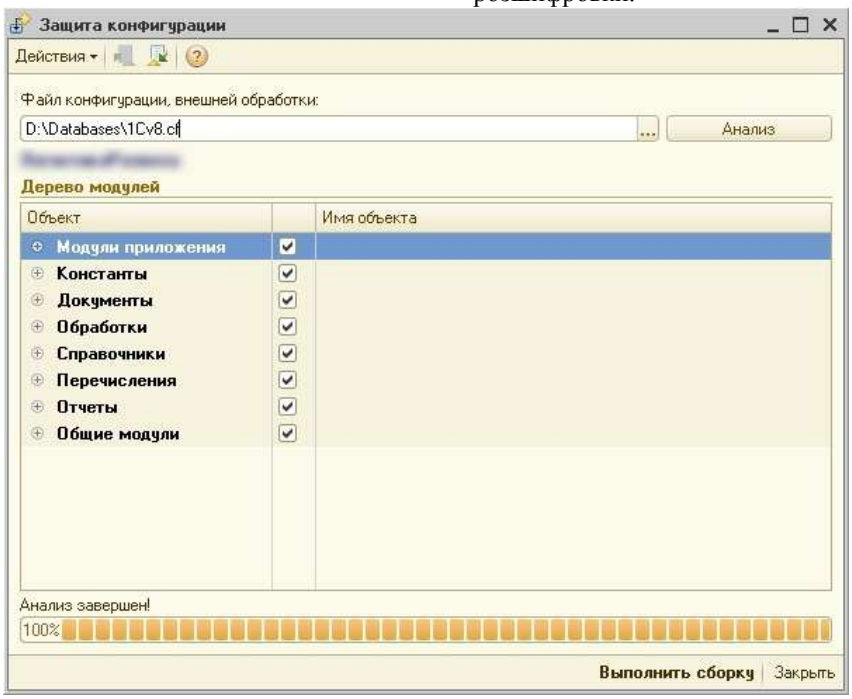

Рис. 1. Захист конфігурації у системі 1С

Злом 1С для SQL зазвичай складається з 2-х стадій.

Перша стадія це дешифрування пароля DBO.

Друга стадія це аналіз даних через пряме підключення до MS SQL за допомогою Microsoft Query і Excel. Друга стадія може полягати і в копіюванні бази, але це роблять рідше.

Слід зазначити, що фахівці з 1С представляючи безнадійність захисту пароля DBO застосували зовсім слабкий метод криптування (Xor-шифрування). Тому дешифрування пароля проводиться дуже легко. Для цього зазвичай намагаються скопіювати файл 1CV7.DBA (для 7 версії) або 1cv8.1cf (для 8 версії) і потім його дешифровують спеціальними програмами, наприклад, unsql.exe. Інший метод не вимагає копіювання файлу, а будується на запуску троянської конфігурації або зовнішнього звіту 1С, які на макромові 1С містять алгоритм дешифрування пароля.

Після отримання пароля DBO зловмисник зазвичай приступає до аналізу даних в базі використовуючи Microsoft Query і Excel.

Скопіювати базу MS SQL не дуже просте заняття, оскільки це не зробити шляхом копіювання файлів. Потрібна спеціальна програма, наприклад Data Migration Wizard, за допомогою якої можна скопіювати базу 1С з SQL у вигляді DBF-файлов собі на диск.

Також слід зазначити, що можливий злом 1С для SQL шляхом аналізу тимчасових файлів, в яких 1С містить значну частину БД.

Треба сказати, що у разі MS SQL адміністратор може розвернути засоби аудиту, які дозволять відмітити несанкціонований доступ до баз з Microsoft Query і копіювальників даних. Це можна зробити використовуючи SQL Profiler. Проте потрібна спеціальна і дуже серйозна настройка профайлера. Інакше можна не відмітити злом серед тисяч легальних команд, і крім того, без настройки профайлер у декілька разів знижує швидкість роботи БД.

MS SQL дозволяє задіяти шифрування при передачі даних через SSL.

Інший важливий момент, це настройка входу в базу не під SA, а під окремим користувачам. Наступна дія, це розділення системи на декілька окремих баз 1С. Такими засобами можна мінімізувати збиток, але в цілому дірки для злому залишаються.

Для вирішення проблем безпеки 1С для SQL потрібно задіювати режим Row Level Security з MS SQL. Проте для цього потрібний спеціальний продукт.

Microsoft Terminal Server користується заслуженою репутацією хорошого рішення, якщо з 1С працюють до 10. У разі використання терміналу користувач працює з програмою не на своїй машині, а на термінальному сервері. Управляє користувач програмою через спеціальне вікно терміналу. Термінал зручний тим, що дозволяє працювати 1С на слабких і старих машинах. Інший аспект терміналу - це можливість підвищити безпеку 1С.

Упевненість багатьох менеджерів в надійності захисту MS Terminal Server тільки полегшує завдання для зловмистників. Злом бази під терміналом також зазвичай полягає в копіюванні бази і подальшому її аналізі.

Наступний момент, ми можемо закрити від користувача непотрібні застосування через засоби NTFS. Проте, як видно вище, користувач може використовувати засоби копіювання фактично ні чого не запускаючи на сервері. Цікавий момент, відключити в 1С панель "Файл" з її Ctrl+o і Ctrl+s не можна. Єдино надійний варіант це закрити файловий порт на термінальному сервері. Але в даному випадку перестане працювати друк по мережі, резервне копіювання на аварійний сервер і так далі. Для невеликої організації це серйозна проблема, оскільки сервер дорога штука і хоче він використовувати багатофункціонально, а для середньої організації відсутність мережевого друку це просто не серйозно. Я вже не говорю про те, що доведеться накласти заборону на використання Microsoft Office спільно з 1С. Інакше, навіть із закритим портом, базу розпатрають на сервері без копіювання. Загалом, чим більше ми відключимо сервісів, тим безпечніше сервер, можна його і взагалі вимкнути, він буде зовсім безпечним, тільки кому він такий потрібний? Для нормальної роботи доведеться відкрити цілий ряд портів: 25, 53, 80, 110, 119 і ін. Все це потенційні дірки в захисті сервера, та і по самому порту терміналу (3389) можна провести атаку класу DOS.

Розмежування доступу користувачів у КІСБО необхідне ще й для того, щоб забезпечити ефективну організацію облікового процесу, юридичну доказовість складених електронних носіїв інформації тощо.

Ми визначили наступну послідовність етапів методики розмежування доступу користувачів:

1) формування структури облікового процесу підприємства;

2) формування організаційної структури КІСБО;

3) розподіл обов'язків між користувачами КІСБО;

4) визначення прав доступу користувачів до функцій програми та інформаційних ресурсів.

Розмежовуючи доступ до функцій та інформаційних ресурсів програми, ми застосували наступні принципи:

- право на проведення операцій ми надали лише головному бухгалтеру і його замісникам: бухгалтеру з податкового обліку та бухгалтеру з обліку доходів, витрат і фінансових результатів. Усі інші працівники лише вводять первинні документи в інформаційну базу без права їх проведення. Тут ми керувалися

потребами суворого контролю за податковими зобов'язаннями, податковими кредитами, ПДВ та доходами, витратами і фінансовими результатами підприємства, які випливають майже з кожного первинного документа;

- право використання звітів і регістрів обліку ми надали теж лише головному бухгалтеру і його замісникам та директору і комерційному директору і мотивуємо це тим, що тільки цим посадовим особам включена в обов'язки підготовка звітів, а також ця міра застосовується з метою обмеження доступу до інформаційних ресурсів підприємства і збереження комерційної таємниці;
- право на формування плану рахунків, типових операцій, операцій, проводок, обробок ми надали лише головному бухгалтеру з метою зосередження елементів організації облікового процесу в єдиних руках. З тією ж метою ми дозволили формувати константи, календарі та визначати користувачів бухгалтерської системи і їх права доступу тільки головному бухгалтеру;
- право видаляти помилкові записи та змінювати проведені документи вважаємо за доцільне надати лише головному бухгалтеру, а іншим посадовим особам – лише право на помітку на видалення і мотивуємо це необхідністю захисту інформації від знищення.

Для виконання типового обсягу робіт, наприклад для торгівельного підприємства, пропонується організаційна структура КІСБО (рис. 2), яка побудована на основі концепції АРМ (автоматизованих робочих місць) трьох рівнів:

АРМ вищих керівників;

АРМ спеціалістів;

АРМ технічних виконавців.

Ця організаційна структура є доцільною в умовах використання мережевих бухгалтерських систем. Визначивши структуру АРМів, ми можемо розподілити функції між окремими робочими місцями. Розподіл функцій між працівниками підприємства повинен здійснюватися з урахуванням основних принципів внутрішнього контролю. Зокрема, з метою забезпечення зловживань доцільно розподілити функції дозволу і введення господарських операцій в інформаційну базу, функції дозволу операцій і зберігання активів, функції проведення операцій в інформаційній базі і зберігання активів, функції введення операцій та їх бухгалтерське проведення, функції обліку відпуску активів та обліку їх оплати, обліку розрахунків та обліку активів тощо.

Рис. 2. Організаційна структура КІСБО підприємства

Аналізуючи можливості розмежування доступу в КІСБО «1С:Підприємство» ми можемо констатувати, що ці можливості є недостатніми для бухгалтерій. Зокрема, коли з одним первинним документом працює більше двох посадових осіб, відповідальних за формування кожний своїх реквізитів, неможливо визначити чи документ пройшов усі стадії обробки і контролю до його проведення. Більш доцільною є реалізація паралельного документообігу в системі, коли кожний документ одночасно може оброблятися декількома особами, зроблені зміни кожним із користувачів об'єднуються на останньому етапі документообігу і документ має позначки про те, які етапи документообігу він пройшов.

Висновки. Таким чином, підводячи підсумки викладеного вище, ми вправі зробити наступні висновки та внести такі рекомендації:

Розмежування доступу до функцій та інформаційних ресурсів бухгалтерської програми необхідне для попередження злочинів службовців, помилок у роботі, встановлення юридичної доказовості складених електронних носіїв інформації, раціональної організації процесу обробки інформації.

Недостатність публікацій та відсутність методичного забезпечення з розмежування доступу користувачів спричинює невикористання підприємствами можливостей програмних продуктів.

1. Нами визначена послідовність етапів запропонованої нами методики розмежування доступу користувачів:

- формування структури облікового процесу підприємства;
- формування організаційної структури КІСБО;
- розподіл обов'язків між користувачами КІСБО;
- визначення прав доступу користувачів до функцій програми та інформаційних ресурсів.

Сформована організаційна структура КІС БО торговельних підприємств в умовах застосування мережевої бухгалтерської системи з виділенням АРМів трьох рівнів (рис.1).

Нами встановлені набори прав користувачів, які дозволять виконувати посадовим особам їх прямі обов'язки і забезпечити підприємствам безпеку та ефективне функціонування КІСБО.

При розмежуванні прав доступу нами впроваджений суворий контроль за валовими доходами, валовими витратами, ПДВ, доходами, витратами і фінансовими результатами та грошовими коштами і матеріальними активами підприємства, захист комерційної таємниці та попередження витоку і знищення та перекручення інформації. Ми зосередили організацію облікового процесу та керування доступом до функцій та інформаційних ресурсів програми в єдиних руках.

Встановлено недоліки функцій розмежування доступу в КІСБО «1С:Підприємство» і запропоновано впровадити паралельний документообіг.

Пропонується з метою захисту інформації, встановлювати доступ працівників з АРМ виконавців тільки до тих об'єктів, за якими у них закріплена матеріальна відповідальність. Для цього необхідно внести відповідні зміни в списки набору прав конфігуратора.

Література

1. Про інформацію: Закон України від 2.10.1992 р. № 1642-III // Галицькі контракти. – 1996. - №47 – с. 44-50.
2. Про захист інформації в автоматизованих системах: Закон України від 5.07.1994 р. № 81//94-ВР. // Галицькі контракти. – 1996. - №47 – с. 44-50.
3. Верига Ю.А. Захист інформації в комп'ютерних інформаційних системах бухгалтерського обліку / Верига Ю.А., Деньга С.М. // Бухгалтерський облік і аудит.- 2004.- № 5.- С. 59-65.
4. Взлом и защита 1С: Предприятия. О проблеме взлома 1С:Предприятия администраторам и пользователям [электронный ресурс] - Режим доступу: http://ivn73.tripod.com/stat_security_admin.htm.

References

1. Pro informaciju: Zakon Ukraïni vid 2.10.1992 r. № 1642-III // Galic'ki kontrakti. – 1996. - №47 – s. 44-50.
2. Pro zahist informacií v avtomatizovanih sistemah: Zakon Ukraïni vid 5.07.1994 r. № 81//94-VR. // Galic'ki kontrakti. – 1996. - №47 – s. 44-50.
3. Veriga Ju.A. Zahist informacií v komp'juternih informacijnih sistemah buhgalters'kogo obliku / Veriga Ju.A., Den'ga S.M. // Buhgalters'kij oblik i audit.- 2004.- № 5.- S. 59-65.
4. Vzlom i zashhita 1S: Predprijatija. O probleme vzloma 1S:Predprijatija administratoram i pol'zovateljam [jelektronnyj resurs] - Rezhim dostupu: http://ivn73.tripod.com/stat_security_admin.htm.

О.П. Рудов, Т.П. Романченко, А.С. Скріпкіна

ІНФОРМАЦІЙНИЙ ЗАХИСТ СИСТЕМИ 1С ПІДПРИЄМСТВО

В статті розглянуті деякі аспекти розмежування доступу користувачів у комп'ютерних системах бухгалтерського обліку, на прикладі «1С:Підприємство», що є необхідним для забезпечення ефективної організації облікового процесу, та надійного захисту комерційної інформації суб'єкту господарювання. Рис. 2., Бібл. 4.

Ключові слова: *захист інформації, інформаційна система, 1С:Підприємство, розмежування доступу.*

A.P. Pudov, T.P. Romanchenko, A.S. Skripkina

INFORMATION PROTECTION SYSTEM 1C: ENTERPRISE

The article deals with some aspects of concurrent access users in computer accounting systems, for example "1C: Enterprise", which is necessary for the efficient organization of the accounting process, and reliable protection of commercial information entity. Fig. 2., Lit. 4.

Keywords: *information security, information systems, 1C: Enterprise, access.*

Рудов Олександр Павлович, к.е.н., доцент, Луганський національний аграрний університет, кафедра економічної кібернетики

Романченко Тетяна Петрівна, ас., Луганський національний аграрний університет, кафедра економічної кібернетики

Скріпкіна Антоніна Сергіївна, ас., Луганський національний аграрний університет, кафедра економічної кібернетики

Рецензент: д.т.н., проф. Лєві Л.І.