УДК 004.056.5

Зотова І. Г.;
Берестов Д. С.;
Кульчицький О. С.;
Грицюк В. В.

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Підсистема захисту інформації від несанкціонованого доступу в ERP-системі

Резюме. У статті розглядаються підсистеми захисту інформації від несанкціонованого доступу до інформаційних ресурсів ERP-системи.

Ключові слова: ERP-система, інформаційна безпека; несанкціонований доступ; захист інформації; підсистема захисту інформації; ідентифікація; аутентифікація; управління доступом до інформації; реєстрація та облік подій; криптографічний захист.

Постановка проблеми. З розвитком інформаційних технологій, які використовуються в *ERP*-системі (англ. *Enterprise Resource Planning*, планування ресурсів підприємства), зростає і складність забезпечення її інформаційної безпеки. Досвід експлуатації *ERP*-систем показує, що незважаючи на тенденцію до підвищення рівня інформаційної захищеності системи вона є досить уразливою з точки зору несанкціонованого доступу до її інформаційних ресурсів. У зв'язку з цим при забезпеченні інформаційної безпеки *ERP*-системи в якості основного джерела загроз розглядається несанкціонований доступ. Тому питання, які пов'язані із захистом *ERP*-системи від несанкціонованого доступу до її інформаційних ресурсів є досить актуальними [1, 2].

Ступінь розробленості проблеми. Створення надійно захищеної ERP-системи від несанкціонованого доступу є надзвичайно складним завданням. При вирішанні цього завдання фахівці керуються принципом, згідно якому захист *ERP*-системи від несанкціонованого доступу повинен організовуватися й ефективно функціонувати в усіх фрагментах системи, в яких циркулює, обробляється і зберігається інформація, яка підлягає захисту. У цих умовах збільшується і кількість різних видів механізмів захисту інформації, які можуть забезпечити захист ERP-системи від несанкціонованого доступу. У відповідності з цими механізмами створюються і відповідні їм підсистеми захисту, які є складовою частиною єдиної системи захисту *ERP*-системи. [1].

Мета статті. Аналіз механізмів підсистем захисту інформації та їх особливостей, які використовуються в ERP-системі для захисту від несанкціонованого доступу.

Виклад основного матеріалу. При вирішені проблеми, щодо забезпечення інформаційної безпеки *ERP*-системи необхідно виходити з того, що вона представляє собою комплекс програмного і апаратного обладнання, з'єднаний в єдиний ланцюг. До складу *ERP*-системи входять сервери, на яких зберігається вся її інформація та чітко структурована інформаційно-телекомунікаційна мережа. Активним обладнанням *ERP*-системи є різні мережеві адаптери. Також до складу *ERP*-системи входять автоматизовані робочі місця (АРМ) користувачів, створених на базі персональних комп'ютерів (ПК), які підключені до серверів до різних інформаційнх служб і системам загального призначення. Робота користувачів із програмним забезпеченням АРМ здійснюється, як правило, через меню.

Крім цього *ERP*-система представляє собою територіально розподілену систему, в якій її інформаційні об'єкти інтенсивно взаємодіють між собою за даними (ресурсами) і управлінням (подіям) локальних обчислювальних мереж та окремих обчислювальних засобів. Зв'язок між ними здійснюється фізично за допомогою мережевих ліній зв'язку (основними з яких є лінії волоконно-оптичного і провідного зв'язку) та програмно за допомогою механізму повідомлень. При цьому управляючи повідомлення і дані, що пересилаються між об'єктами *ERP*-системи, передаються у вигляді пакетів обміну. Тому необхідно враховувати наявність мережевих ліній зв'язку *ERP*-системи як на контрольованій, так і на неконтрольованої території. Також через недоліки сучасних інформаційних технологій, які використовуються в *ERP*-системі, а також неухильне зростання

складності програмно-апаратних засобів самої системи, кількість інформаційних загроз її безпеці і способів їх реалізації постійно збільшується.

Виходячи із зазначеного вище слідує, що забезпечення інформаційної безпеки *ERP*-системи потрібує не тільки здійснення деякої сукупності науково-технічних і організаційних заходів, застосування специфічних засобів і методів захисту, а й створення цілісної системи захисту інформації, яка базується на чіткій організації і регулярному управлінні.

Забезпечення інформаційної безпеки *ERP*-системи ґрунтується на глибокому аналізі негативних наслідків від впливу на неї різних видів інформаційних загроз. При проведені такого аналізу, як правило, розглядається три базові категорії інформаційних загроз, які можуть впливати на інформаційні ресурси і процеси *ERP*-системи, а саме [3, 4]:

відмови і збої в апаратних засобах системи, аварійні ситуації та інші події без участі людини;

помилкові або ненавмисні дії обслуговуючого персоналу та абонентів системи;

несанкціонований доступ (НСД) до інформації.

Однією з найбільш поширених і різноманітних інформаційних загроз, які можуть завдати суттєву шкоду інформаційній безпеці *ERP*-системі є НСД до інформації. Де під терміном "інформація" в *ERP*-системі розуміються такі види інформації:

для управління та прийняття рішень (тобто інформація користувачів);

забезпечення управління обладнанням *ERP*-системи;

забезпечення управління і роботи засобів захисту;

забезпечення реалізації всіх технологій обробки інформації в ERP-системі.

При цьому захисту від НСД підлягають всі перераховані види інформації.

До НСД в *ERP*-системі можна віднести [5]:

проникнення в операційну середу *ERP*-системи з використанням штатного програмного забезпечення (засобів операційної системи або прикладних програм загального застосування);

створення позаштатних режимів роботи програмних (програмно-апаратних) засобів за рахунок навмисних змін службових даних, ігнорування передбачених у штатних умовах обмежень на склад і характеристики оброблюваної інформації, спотворення самих даних тощо;

впровадження шкідливих програм.

Також можливе поєднання зазначених вище загроз. Наприклад, за рахунок впровадження шкідливих програм можуть створюватися умови для НСД в операційну середу *ERP*-системи.

При вирішенні питання щодо захисту інформації від НСД в *ERP*-системі використовуються такі захисні механізми як:

ідентифікація та аутентифікація користувачів або процесів;

розмежування доступом до інформаційних ресурсів системи;

реєстрація та облік подій, які відбуваються в системі;

криптографічний захист інформації в системі

У відповідності з цими механізмами створюються ї відповідні їм підсистеми захисту які є складовою частиною єдиної системи захисту *ERP*-системи.

Підсистема ідентифікації призначена для розпізнання користувачів і процесів в *ERP*-системі за допомогою присвоєного їм індивідуального імені або особистого коду, який перевіряється підсистемою, чи зареєстрований він у базі даних. Вона дозволяє спростити процедуру виділення конкретного користувача або процес із безлічі однотипних. Підсистема ідентифікації забезпечує виконання таких функцій як:

встановлення автентичності та визначення повноважень користувача або процесу при його допуск в систему;

контролювання встановлених повноважень в процесі сеансу роботи;

реєстрація дій користувача.

Підсистема аутентифікації призначена для підтвердження достовірності ідентифікації як користувача, так і процесу або об'єкта системи. Мета аутентифікації користувача або процесу - переконатися в тому, що користувач або процес є саме тим, ким ідентифікувався. Якщо в процесі аутентифікації справжність користувача або процесу встановлена, то система захисту інформації повинна визначити його повноваження. Це необхідно для подальшого контролю та розмежування доступу до інформаційних ресурсів *ERP*-системи. У цій підсистемі можуть використовуватися методи аутентифікації, що засновані на:

використані паролів;

використані жетонів, електронних карток тощо;

вимірі біометричних параметрів людини;

інформації, асоційованої з користувачем, наприклад, з його координатами.

Найбільш поширене розповсюдження получив метод аутентифікації, заснований на паролях. Так, наприклад, у більшості *ERP*-систем використовуються багаторазові паролі. У цьому випадку пароль користувача не змінюється від сеансу до сеансу протягом встановленого адміністратором системи часу його дійсності. Це спрощує процедури адміністрування, але підвищує загрозу розкриття пароля.

Можливості засобів аутентифікації за рівнем інформаційної безпеки класифікують на три категорії [6]:

статична аутентифікація;

стійка аутентифікація;

постійна аутентифікація.

Перша категорія забезпечує захист від НСД у системах, де порушник не може під час сеансу роботи прочитати аутентифікаційну інформацію. Прикладом засобів статичної аутентифікації є традиційні постійні паролі. Їх ефективність залежить від того наскільки добре вони захищені.

Друга категорія використовує динамічні дані аутентифікації, що змінюються з кожним сеансом роботи. Реалізаціями стійкої аутентифікації є системи, що використовують одноразові паролі та електронні підписи. Однак стійка аутентифікація не забезпечує захист від активних атак, в ході яких порушник може оперативно (протягом сеансу аутентифікації) перехопити, модифікувати і вставити інформацію в потік переданих даних.

Третя категорія забезпечує ідентифікацію кожного блоку переданих даних, що охороняє їх від несанкціонованої модифікації або вставки. Прикладом реалізації зазначеної категорії аутентифікації є використання алгоритмів генерації електронних підписів для кожного біта інформації що пересилається.

Підсистема управління доступом до інформації в *ERP*-системі, виконує одну з основних функцій в захисті інформації від НСД. Під доступом до інформації ERP-системи розуміється такий порядок використовування її інформаційних ресурсів, при якому користувач, процес, програма отримають доступ до приладів, дисків, файлів системи у відповідності з встановленими правилами. Підсистема управління доступом до інформації – це програмно-апаратний комплекс, який не входить до ядра операційної системи і виконує функції захисту від НСД серверів, АРМ користувачів і прикладних сервісів. Крім цього, вона забезпечує захист від НСД апаратно-програмних засобів, що впливають на функціонування сегментів інформаційних мереж, в яких обробляється інформація.

При створенні підсистеми управління доступом можуть використовуватися як накладні, так і вбудовані в операційні системи й додатки системи захисту від НСД. Доступ до інфраструктурних і інформаційних ресурсів, які захищаються, повинен здійснюватися у відповідності з матрицею доступу. При створенні матриці доступу для інфраструктурних ресурсів здійснюється ідентифікація терміналів, серверів, вузлів мережі, каналів зв'язку, периферійних приладів - за логічними ім'ями, адресами в інформаційній мережі, унікальними кодами приладів, цифровими сертифікатами та іншими технологічно допустимими параметрами. Для інформаційних ресурсів повинна здійснюватися ідентифікація сервісів, програм, файлів, - за мережевими адресами доступу до них, логічними іменами, цифровими сертифікатами та іншими технологічно допустимими параметрами.

Крім цього користувачі ідентифікуються за логічним ім'ям, паролям, цифровим сертифікатам, електронним ключам та іншим параметрам. Набір ідентифікаторів користувача, необхідний для надання йому доступу до кожного окремого інфраструктурного або інформаційного ресурсу, визначається на стадії технічного проектування підсистеми захисту інформації і включає: логічне ім'я, пароль, цифровій сертифікат або електронний ключ. Передача ідентифікаційних параметрів здійснюється по захищеним каналам зв'язку.

Підсистема реєстрації та обліку подій здійснює реєстрацію та облік подій, які відбуваються в системі та дії користувачів. Реєструється час події, джерело і ці події. Події зберігаються в спеціальній базі даних для послідуючого аналізу і статистичної обробки. Також реєструються і критичні події, такі як спроби порушення прав доступу до приладів, дисків, файлів. Адміністратор визначає рівень критичності подій, режим оповіщення, а також дії, які необхідно виконати при появі таких подій.

Облік подій здійснюється для підтримки безпеки в мережі *ERP*-системи. Це дозволяє відстежувати дії користувачів, а також дії операційної системи. Засобами підсистеми можна задати режим, при якому операційна система буде реєструвати події в журналі безпеки. У ньому зберігаються записи про успішні і невдалі спроби входу в *ERP*-систему а також про такі події, як створення, відкриття і закриття файлів або інших одиниць інформаційного ресурсу *ERP*-системи.

Підсистема криптографічного захисту інформації – призначена для виключення НСД до інформаційних ресурсів *ERP*-системи. Вона за допомогою надійних криптографічних алгоритмів перетворює інформацію в усіх фрагментах *ERP*-системи, в яких циркулює, обробляється і зберігається інформація. Підсистема криптографічного захисту в *ERP*-системі може виконувати наступні функції [7, 8]:

здійснювати захист від НСД до інформації, розташованої на дискових носіях;

здійснювати захист від НСД до інформації, яка передається по каналах зв'язку системи ;

здійснювати управління ключовою інформацією.

У підсистемі криптографічного захисту *ERP*-системи можуть використовуватися апаратні, програмні або програмно-апаратні атестовані (сертифіковані) засоби криптографічного захисту, які реалізують криптографічні функції захисту інформації.

Основною особливістю апаратних засобів криптографічного захисту інформації (АЗКЗІ) є апаратна реалізація основних криптографічних функцій (криптографічних перетворень, управління ключами, криптографічних протоколів тощо) за рахунок створення і застосування спеціалізованих процесорів. АЗКЗІ використовуються в ERP-системі, коли є потреба максимально підвищити рівень її інформаційного захисту від НСД але при цьому вони повинні мати досить високу продуктивність криптографічних операцій.

Також криптографічні функції захисту можуть бути реалізовані у вигляді ПЗКЗІ. Переваги такої реалізації: ПЗКЗІ легко копіюються, вони прості у використанні, їх неважко модифікувати відповідно до конкретних потреб. Поряд із цими перевагами у ПЗКЗІ є й істотні недоліки. ПЗКЗІ є більш уразливими ніж АСКЗІ оскільки їх програми, які реалізують криптографічні функції захисту інформації, можуть бути досить просто модифіковані злочинцем. У зв'язку з цим ПЗКЗІ використовуються для захисту інформації в *ERP*-системі, яка не містить закритої інформації.

В *ERP*-системі частіше застосовуються програмно-апаратні засоби, криптографічного захисту інформації тому, що вони поєднують у собі гнучкість програмного рішення з надійністю апаратного. При цьому за рахунок гнучкої програмної компоненти можливо швидко міняти інтерфейс користувача, кінцеві функції продукту, робити його кінцеве настроювання; а апаратна компонента дозволяє захистити від модифікації алгоритм криптографічного примітива, забезпечити високу захищеність ключового матеріалу і найчастіше більш високу швидкість роботи.

Висновки. Розглянуті підсистеми складають базис для формування системи захисту інформації від несанкціонованого доступу *ERP*-системи в разі використання її, як інтеграційної платформи для автоматизації адміністративно-господарської діяльності підприємства. Необхідність та достатність використання розглянутих підсистем залежить від моделі загроз та моделі порушника об’єкта автоматизації, політики безпеки підприємства та техніко-економічних можливостей по їх впровадженню.

Напрями подальших наукових досліджень. Подальші наукові дослідження доцільно зосередити на необхідності уточнення та обґрунтування достатності застосовуваних засобів захисту, оптимізації системи захисту інформації, підвищення її ефективності шляхом обґрунтованого вибору показників ефективності, критеріїв оцінки і методів оцінювання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.

1. Зырянов Ю. Информационная безопасность ERP-систем. – Режим доступа: *http://www. citcity.ru/16501/*.
2. Сердюк В. А. Уязвимость и информационная безопасность ERP-систем. – Режим доступа: *http://www.connect.ru/article.asp?id=3167*.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. и доп. - М.:Радио и связь, 2001. - 376 с.
4. Шевченко В.Л. Несанкціонований доступ до інформаційних ресурсів ERP-системи / В.І. Кулажський, О.С. Кульчицький// ЦВСД НУО України, м.Київ, ЗНП ЦВСД НУО України, Вип. 1(50), С. 9, 2014 р.
5. Проблема защиты информации в ТКС. – Режим доступу: *library.tuit.uz/skanir_knigi/book/informacionnaya/glav_3_4.htm*.
6. Идентификация и аутентификация - Режим доступу: http://sernam.ru/ss_23.php.
7. Жданов О.Н. Методы и средства криптографической защиты: учеб. пособие / О.Н Жданов, В. В. Золотарев; СибГАУ. – Красноярск, 2007. – 217 с.
8. Яковлев А.В. Криптографическая защита информации: учеб. пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с..

Стаття надійшла до редакції 29.09.2015

Зотова И. Г.;
Берестов Д. С.;
Кульчицкий О. С.;
Грицюк В. В.
Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Подсистема защиты информации от несанкционированного доступа в ERP-системе

Резюме. В статье рассматриваются подсистемы защиты информации от несанкционированного доступа к информационным ресурсам ERP-системы.

Ключевые слова: ERP-система; информационная безопасность; несанкционированный доступ; защита информации; подсистема защиты информации; идентификация; аутентификация; управление доступом к информации; регистрация и учет событий; криптографическая защита.

I. Zotova;
D. Berestov;
A. Kulchizkiy;
V. Gritsyuk
Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovskij, Kyiv

Subsystem of priv from an unauthorized division in ERP-system

Resume. This article discusses the security subsystems from unauthorized access to information resources ERP-system.

Keywords: ERP-system; information security; unauthorized access; protection of information; security subsystem information; identification; authentication; control access to information; registration and recording of events; cryptographic protection.