УДК 004.056.5
Шевченко В.Л., д.т.н., с.н.с.[1];
Кулажський В.І., к.т.н., доцент[2];
Кульчицький О.С.[2]

[1] - Державний університет телекомунікацій;
[2] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського

Несанкціонований доступ до інформаційних ресурсів ERP-системи

Резюме. Розглянуто механізми несанкціонованого доступу до інформаційних ресурсів ERP-системи та особливості самої системи, які необхідно враховувати при забезпечені її захисту.

Ключові слова: інформаційна безпека**,** інформаційна загроза**,** інформація, несанкціонований доступ, ERP-система, інформаційні ресурси, захист, мережа.

Несанкционированный доступ к информационным ресурсам ERP-системы

Резюме. Рассмотрены механизмы несанкционированного доступа к информационным ресурсам ERP-системы, а также особенности самой системы, которые необходимо учитывать при обеспечении ее защиты.

Ключевые слова: информационная безопасность, информационная угроза, информация, несанкционированный доступ, ERP-система, информационные ресурсы, ,защита, сеть.

Unauthorized access to informational resources of ERP-system

Resume. In the article are considered the mechanisms of unauthorized access to informational resources of the ERP-system as well as features of the system that must be considered while ensuring its protection.

Keywords: informational security, informational threat, information, unauthorized access, ERP-system, informational resources, protection, network.

Постановка проблеми. З використанням в інформаційно-телекомунікаційних системах новітніх інформаційних технологій зазнали змін як методи, так і способи ведення сучасних інформаційних війн. У цих умовах проблема інформаційної безпеки ERP-системи стає досить актуальною. Важливість її рішення обумовлюється необхідністю уточнення і обґрунтування достатності застосовуваних заходів захисту інформації, оптимізації систем захисту, підвищення ефективності контролю безпеки інформації в ERP-системі.

Однією з найбільш поширених і різноманітних інформаційних загроз, яка може завдати суттєвої шкоди інформаційній безпеці ERP-системи є несанкціонований доступ (НСД) до її інформаційних ресурсів. Досвід експлуатації ERP-системи показує, що незважаючи на тенденцію до підвищення рівня її інформаційної захищеності, а також через постійне розширення її інформаційно-телекомунікаційних мереж, вона є досить уразлива з точки зору НСД. У зв'язку з цим захист ERP-системи від НСД до її інформаційних ресурсів розглядається як складова частина загальної проблеми забезпечення інформаційної безпеки ERP-системи.

Ступінь розробленості проблеми. ERP-система представляє собою територіально розподілену інформаційно-телекомунікаційну систему, в якій інформаційні об'єкти здійснюють управління локальними обчислювальними мережами, власними обчислювальними засобами та взаємодіють між собою стосовно обміну інформацією. В ERP-системі може використовуватися як вітчизняне, так і імпортне програмне забезпечення, яке працює на імпортних обчислювальних засобах та реалізує сучасні інформаційні технології. Через неухильне зростання складності програмно-апаратних засобів ERP-системи кількість шляхів та способів за якими може здійснюватися НСД до її інформаційних

ресурсів постійно збільшується і, отже, збільшується і кількість необхідних для його нейтралізації засобів захисту. Тому питання, пов'язані із захистом інформаційних ресурсів ERP-системи від НСД, є досить актуальними [1, 2, 3].

Мета статті. Аналіз механізмів за якими може здійснюватися НСД до інформаційних ресурсів ERP-системи та особливостей самої системи, які необхідно враховувати при забезпечені її захисту.

Виклад основного матеріалу. Як показали наукові дослідження та практичний досвід, для забезпечення інформаційної безпеки ERP-системи потрібне не тільки здійснення певної сукупності науково-технічних і організаційних заходів та застосування специфічних засобів і методів захисту, а й створення цілісної системи захисту інформації, яка базується на чіткій організації і регулярному управлінні. При цьому керуються основним принципом, згідно з яким система захисту інформації має ефективно функціонувати на всіх етапах її існування і в усіх фрагментах ERP-системи, в яких циркулює, обробляється і зберігається інформація, що підлягає захисту.

Забезпечення інформаційної безпеки ERP-системи ґрунтується на глибокому аналізі негативних наслідків впливу на неї різних видів інформаційних загроз. При проведені такого аналізу, як правило, розглядаються наступні категорії інформаційних загроз:

– відмови і збої в апаратних засобах системи, аварійні ситуації та інші події які відбуваються, без участі персоналу;

– помилкові або ненавмисні дії обслуговуючого персоналу та користувачів системи;

– НСД порушниками до інформаційних ресурсів системи.

Однією з найбільш поширених і різноманітних інформаційних загроз, які можуть завдати суттєву шкоду інформаційній безпеці ERP-системи є НСД до її інформаційних ресурсів. Під терміном "інформаційні ресурси" розуміється інформація, яка циркулює, обробляється і зберігається в ERP-системі, а саме, інформація для:

- управління та прийняття рішень;
- управління обладнанням ERP-системи;
- управління і роботи засобів захисту системи;
- реалізації технологій обробки інформації в ERP-системі.

Для ефективного захисту ERP-системи від НСД до її інформаційних ресурсів необхідний ретельний аналіз можливих шляхів, за якими він може здійснюватися, що дозволяє своєчасно вжити необхідні заходи захисту. До можливих шляхів НСД до ERP-системи можна віднести [4, 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 інформації, яка забезпечує реалізацію всіх технологій обробки інформації в ERP-системі;
- впровадження шкідливих програм.

Крім того, можливе поєднання зазначених вище шляхів НСД. Наприклад, за рахунок впровадження шкідливих програм можуть створюватися умови для НСД в операційну середу ERP-системи.

Несанкціонований доступ до інформаційних ресурсів ERP-системи є реалізацією навмисної загрози її інформаційній безпеці і має назву *інформаційна атака*. Враховуючи сучасну тенденцію щодо підключення ERP-системи до єдиного інформаційного простору, слід чекати різкого зростання таких атак на систему з метою пошкодження її інформаційних ресурсів. Для забезпечення надійного захисту ERP-системи від інформаційних атак необхідно враховувати те, що НСД до її інформаційних ресурсів може здійснюватися як активно, так і пасивно.

При *активному НСД* можна змінювати інформацію, яка циркулює, обробляється і зберігається в ERP-системі, тобто, вибірково підміняти, модифікувати, додавати інформацію або змінити порядок її проходження по інформаційно-телекомунікаційним каналам. Можна також анулювати або затримати на деякий час проходження інформації з того чи іншого інформаційного об'єкта ERP-системи.

При *пасивному НСД* можна лише спостерігати за проходженням інформації по інформаційно-телекомунікаційним каналам ERP-системи, не втручаючись ні в інформаційний потік, ні у зміст переданої інформації. Також можна визначати пункти призначення та ідентифікатори або тільки факт проходження інформації, її довжину і частоту обміну, якщо зміст інформації не розпізнається, тобто здійснювати аналіз трафіку. Інформація та дані, що отримані в результаті такого аналізу, можуть бути використані для активного НСД до інформаційних ресурсів ERP-системи.

Основною метою НСД до інформаційних ресурсів ERP-системи є [6]:

- спостереження за виконанням інформаційних процесів;
- внесення змін в інформацію;
- ліквідація інформації;
- введення хибної інформації;
- затримка інформації;
- запис інформації;
- зміна маршруту передачі інформації;
- дублювання раніше переданої інформації.

Безпосередньо процес НСД до інформаційних ресурсів ERP-системи здійснюється у два етапи:

- збір відомостей про ERP-систему та її систему захисту;
- виконання спроб входження в ERP-систему.

Використання великого числа зв'язаних між собою різних типів інформаційних об'єктів ERP-системи породило велику різноманітність пакетів програм і аналізаторів каналів, за допомогою яких стає можливим виявлення протоколів, які використовуються. Тому доцільно видавати як можна менше інформації про саму ERP-систему до моменту ідентифікації користувача і надання йому права доступу в систему, оскільки, дізнавшись про основний формат входження в мережу, порушник починає експериментувати з різними паролями, визначати імена і намагатися зруйнувати захист.

Після збору відомостей про ERP-систему та її систему захисту здійснюється безпосереднє вторгнення до її інформаційних ресурсів. Номенклатура і кількість використовуваних при цьому засобів втручання залежить від обсягу інформації про ERP-систему, її достовірності та різниці в часі між її отриманням і спробами входу в ERP-систему. Для здійснення НСД в ERP-систему, необхідно мати доступ до її комп'ютерів, інформаційно-телекомунікаційних каналів, протоколи роботи, опис процедур входження в ERP-систему, коди користувачів та паролі. Одним із способів ідентифікації системи є автоматичний перебір можливих комбінацій IP-адрес.

При НСД ідентифікатори користувача можуть відігравати роль допоміжних засобів входження в ERP-систему, оскільки легко обчислюються. Тому ці ідентифікатори надалі краще використовувати як засоби адміністративного контролю та обліку. Найбільш складним при здійсненні НСД до інформаційних ресурсів ERP-системи є добування паролів. Іноді ця задача може бути легко виконана внаслідок поганої організації процедури видачі дозволів на доступ до баз даних ERP-системи. Значно полегшує здійснення НСД до інформаційних ресурсів ERP-системи недбале ставлення користувачів до зберігання паролів і ключів. Крім того, недоліки самих паролів також дають можливість їх розкриття при наборі пароля на клавіатурі, при помилкових виправленнях, у процесі роздачі паролів, під час заміни загубленого пароля, а також за відсутності реєстрації порушень при входженні, або коли однаковий пароль використовується неодноразово в одній і тій же мережі для різних користувачів.

Створення надійно захищеної ERP-системи є надзвичайно складним завданням. Під *надійно захищеною ERP-системою*, у контексті цієї статті, розуміється система, яка забезпечує стійке виконання заходів щодо її захисту у рамках заданого переліку шляхів і способів НСД. Складність цього завдання обумовлена тим, що ERP-система є територіально розподіленою системою, в якій НСД до її інформаційних ресурсів може здійснюватися, не тільки по каналах локальних інформаційних систем, але і по каналах, наявність яких обумовлено специфічними особливостями самої системи, а саме [7]:

- територіальний розподіл інформаційних об'єктів системи і наявність інтенсивного обміну інформацією між ними;
- широкий спектр способів подання, зберігання і протоколів передачі інформації, що використовується;
- інтеграція даних різного призначення, що належать різним суб'єктам, у рамках єдиних баз даних і, навпаки, розміщенням необхідних деяким суб'єктам даних у різних віддалених вузлах мережі;
- абстрагування власників даних від фізичних структур та місця розміщення даних;
- використання режимів розподіленої обробки даних;
- участь у процесі автоматизованої обробки інформації великої кількості користувачів і персоналу різних категорій;
- безпосередній і одночасний доступ до інформаційних ресурсів великої кількості користувачів різних категорій;
- високий ступінь різнорідності засобів обчислювальної техніки і зв'язку, а також їх програмного забезпечення;
- відсутність спеціальних засобів захисту більшості типів технічних засобів, які використовуються в системі.

Так само, необхідно враховувати, що ERP-система включає в себе такі структурні елементи, як:

- локальні та розподілені обчислювальні мережі, які створюються на інформаційних об'єктах ERP-системи та шлюзові засоби розмежування та контролю доступу;

- мережу інформаційно-телекомунікаційних каналів, яка призначена для забезпечення обміну інформацією між інформаційними об'єктами ERP-системи ;

- мережу єдиного інформаційного простору, яка призначена для забезпечення потреб сторонніх користувачів.

Перераховані структурні елементи ERP-системи у процесі функціонування, активно взаємодіють між собою, тому НСД до її інформаційних ресурсів може бути здійснений через будь-який з них.

Крім того, складність завдання щодо створення надійно захищеної ERP-системи від НСД обумовлена різноманіттям можливих видів фізичного представлення інформації в самій системі, наприклад, у вигляді:

- тексту або графічних зображень на папері, моніторах обчислювальних засобів;

- змін стану носіїв інформації, наприклад, магнітних та CD-дисків, Flash-носіїв;

- електричних сигналів у технічних засобах ERP-системи, що обробляють, зберігають або передають інформацію, і в інформаційно-телекомунікаційних каналах, що їх з'єднують.

Усі зазначені вище механізми несанкціонованого доступу до інформаційних ресурсів ERP-системи та особливості самої системи зумовлює наявність широкого спектра можливих шляхів НСД до її інформаційних ресурсів, які при побудові системи захисту інформації повинні бути надійно перекриті з урахуванням аналізу ризику, ймовірностей їх реалізації та обґрунтованих витрат на її створення.

Висновки

1. Забезпечення інформаційної безпеки ERP-системи ґрунтується на аналізі негативних наслідків впливу на неї різних видів інформаційних загроз. Однією з найбільш поширених і різноманітних інформаційних загроз, які можуть завдати суттєву шкоду інформаційній безпеці ERP-системі є НСД до її інформаційних ресурсів.

2. Для ефективного захисту ERP-системи від НСД здійснено аналіз шляхів за якими він може здійснюватися, що дозволяє своєчасно вжити необхідні заходи і засоби для його протидії. При цьому враховується, що НСД до інформаційних ресурсів системи може здійснюватися як активно, так і пасивно.

3. Складність створення надійно захищеної ERP-системи від НСД обумовлена тим, що вона є територіально розподіленою системою, в якій НСД до її інформаційних ресурсів може здійснюватися, не тільки по каналах притаманним для локальних інформаційних систем, але і по каналах, наявність яких обумовлено специфічними особливостями самої системи.

Напрямки подальших наукових досліджень. Інформаційні технології які використовуються в ERP-системі постійно удосконалюються, у зв'язку з чим удосконалюються і способи, за якими може здійснюватися НСД до її інформаційних ресурсів. Тому подальші наукові дослідження доцільно зосередити на розробці відповідних засобів захисту інформації.

СПИСОК ЛІТЕРАТУРИ

1. А.П. Баранов Проблемы обеспечения информационной безопасности в информационно-телекоммуникационной системе специального назначения и пути их решения. – Режим доступа: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/12ccdaa5fd89de1fc32575bd003e2eb1.
2. Зачем необходимо защищать ERP-систему и как это сделать. – Режим доступа: http://ko.com.ua/zachem_neobhodimo_zashhishhat_erp-sistemu_i_kak_jeto_sdelat_88529.
3. 3.Зырянов Ю. Информационная безопасность ERP-систем. – Режим доступа: *http://www.citcity.ru/16501/.*
4. Коханович Г.Защита информации в телекоммуникационных системах.- М.: МК-Прес, - 2005. – 123 с.
5. Герасименко В.А. Основы защиты информации / В.А.Герасименко, А.А.Малюк. – М.:МОПО РФ, МИФИ, 1997, - 537 с.
6. 6 Проблема защиты информации в ТКС. – Режим доступа: library.tuit.uz/skanir_knigi/book/informacionnaya.../glav_3_4.htm
7. 7. Угрозы информационной безопасности в АС. – Режим доступа: http://asher.ru/security/book/its/05.