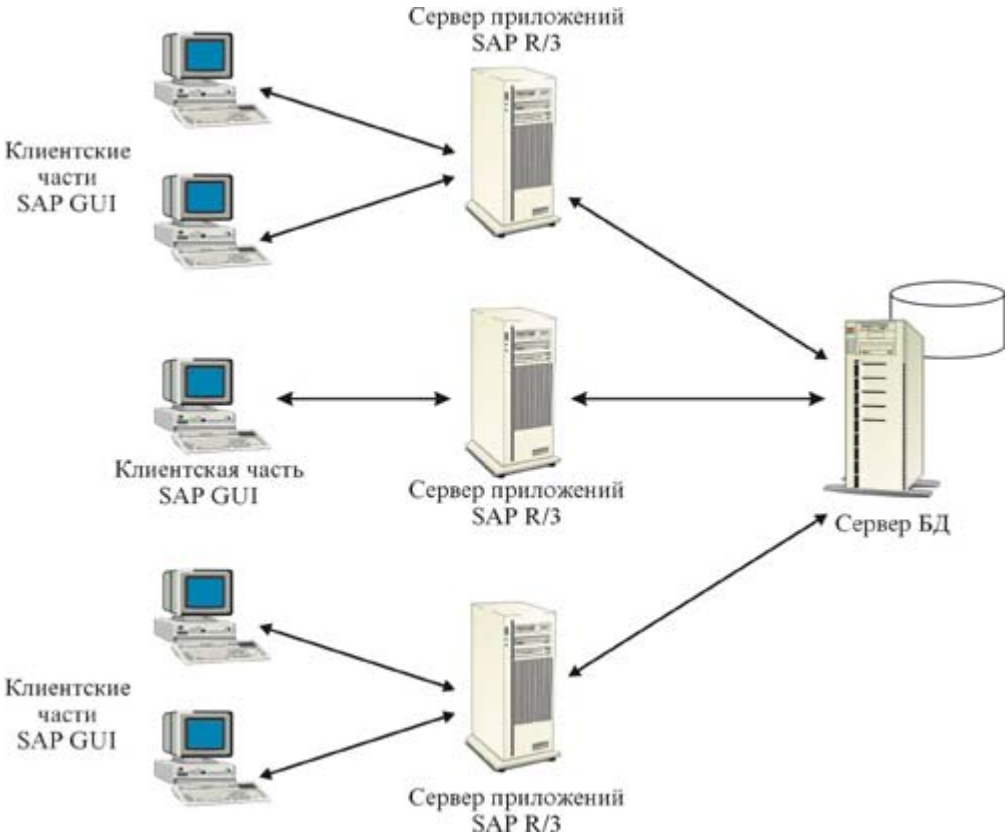
914 гр. Агеенко М.В.

ЗАЩИТА ERP-СИСТЕМ

Прежде чем приступить к анализу мер защиты информации, предусмотренных в ERP-системах, стоит определить базовый перечень угроз, которым они могут подвергаться, и возможные последствия от их реализации.

Нарушение конфиденциальности данных, передаваемых между компонентами ERP-системы. Данный тип угроз может быть реализован нарушителем путем перехвата и анализа сетевого трафика, передаваемого по каналам связи сетей передачи данных. Конфиденциальность может быть нарушена при передаче как по общедоступным каналам связи (например, по каналам связи сети Интернет), так и по каналам внутрикорпоративной сети связи. Угрозы данного типа могут быть обусловлены отсутствием в стандартных стеках сетевых протоколов встроенных средств шифрования.



Несанкционированное искажение данных, передаваемых между компонентами ERP-системы.
Нарушение целостности информации может иметь место при искажении нарушителем содержимого заголовков и полей данных пакетов, передаваемых между компонентами системы. В стандартных стеках протоколов отсутствуют встроенные средства защиты от несанкционированных действий, направленных на искажение передаваемых данных.

Получение несанкционированного доступа к информации, хранимой в БД ERP-системы.
Данный тип нарушений бывает двух видов: с консоли управления базами данных (БД) и посредством удаленной атаки, направленной на несанкционированное ознакомление с содержимым БД.

Нарушение целостности данных, хранимых в БД ERP-системы.
Данный тип угроз аналогичен угрозам предыдущего класса.

Угроза отказа одного из субъектов ERP-системы от совершенных им действий по отправке или получению информации.
Она может возникнуть в процессе обмена информацией между компонентами ERP-систем через установленное сетевое соединение.

Нарушение работоспособности серверов ERP-системы.
Такая угроза может появиться при информационной атаке нарушителя, использующего уязвимость программного и аппаратного обеспечения, на основе которого построена ERP-система.

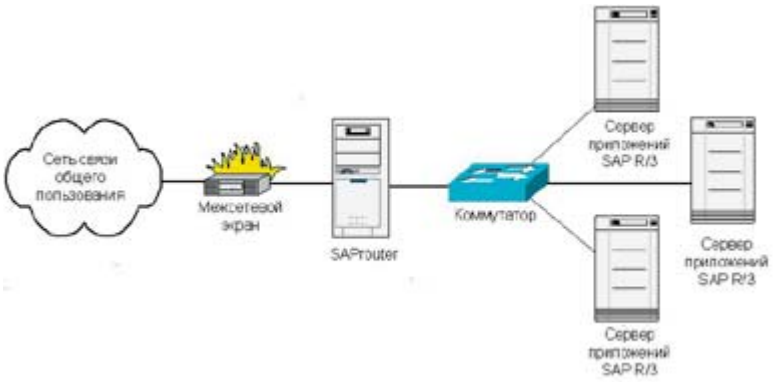
Приведенный перечень угроз показывает, что базовыми объектами защиты ERP-систем являются:

• информация, передаваемая между компонентами ERP-системы;
• информация, хранимая в БД ERP-системы;
• информационно-аналитические серверы ERP-системы;
• другие объекты инфокоммуникационной системы предприятия, нарушение безопасности которых может привести к возникновению угроз для ERP-системы (например, серверы приложений, установленные в корпоративной сети, несанкционированый доступ к которым позволит нарушителю беспрепятственно атаковать компоненты инфраструктуры ERP-системы и др.).

Рассмотрим методы и средства обеспечения информационной безопасности, заложенные разработчиками в ERP-системы, на примере системы SAP R/3, которую разработала немецкая компания SAP AG (System Analyse und Programmentwicklung). Наряду с Oracle, PeopleSoft, J.D. Edwards и другими она входит в число мировых лидеров-производителей.

Система SAP R/3 включает в себя три базовые группы структурных компонентов: клиентское ПО SAPgui, серверы приложений SAP R/3 и сервер БД (. SAP R/3 поддерживает следующие типы СУБД: Oracle, DB2, MS SQL Server, INFORMIX и SAP DB. Все компоненты системы SAP R/3 могут быть территориально распределены и взаимодействуют между собой по удаленным каналам связи. Система SAP R/3 имеет встроенный комплекс средств безопасности, состоящий из четырех базовых подсистем: SSF (Secure Store & Forward), защиты сетевых соединений SNC (Secure Network Communication), аудита (Audit Information System), идентификации и аутентификации.

Рассмотрим каждую из них более подробно.



Защита электронных документов

Подсистема SSF предназначена для обеспечения защиты электронных документов, циркулирующих в системе. Реализуется при помощи двух механизмов — электронной цифровой подписи (digital signature) и электронного цифрового конверта (digital envelope), основанных на инфраструктуре открытых ключей PKI (Public Key Infrastructure), которая, в свою очередь, базируется на технологии асимметричного шифрования. Асимметричное шифрование предполагает наличие двух криптографических ключей — открытого и закрытого, обладающихследующими свойствами:

- ключи могут существовать только в парах «открытый ключ — закрытый ключ». При этом одному открытому ключу может соответствовать только один закрытый;
- доступ только к открытому ключу не позволяет вычислить значение закрытого ключа;
- открытый ключ может свободно распространяться по общедоступным каналам связи, а закрытый должен храниться в секрете.

Форматы данных, используемые подсистемой SSF в процессе формирования цифровых подписей и конвертов, соответствуют стандарту PKCS#7. В стандартной комплектации SAP R/3 подсистема SSF реализуется при помощи вспомогательной библиотеки SAPSECULIB (SAP Security Library), которая использует нестойкие криптографические функции для защиты информации и не поддерживает механизм цифровых конвертов. Для реализации полнофункциональной подсистемы SSF необходимо использовать внешние библиотеки, реализующие криптографические функции защиты заданной стойкости. Взаимодействие между подсистемой и внешними библиотеками осуществляется на основе интерфейса прикладного программирования SSF API. Система SAP R/3 позволяет воспользоваться одновременно несколькими внешними библиотеками с различными криптографическими функциями защиты. Дополнительно для взаимообмена открытыми ключами между пользователями системы могут задействоваться удостоверяющие центры (Certification Authority), которые обеспечивают распределение сертификатов, содержащих открытые ключи пользователей системы. Сертификаты, распределяемые удостоверяющим центром, подписываются электронной подписью этого центра. Как правило, формат сертификата соответствует рекомендациям Международного союза по электросвязи X.509v3.

Защита сетевых соединений между компонентами ERP-системы

Второй базовой подсистемой, при помощи которой реализуются встроенные функции защиты SAP R/3, является подсистема SNC, предназначенная для организации защищенных сетевых соединений, которые устанавливаются между компонентами SAP R/3. Подсистема SNC позволяет осуществлять аутентификацию субъектов, устанавливающих соединение, а также обеспечивать конфиденциальность и целостность данных, передаваемых в рамках установленного соединения. Все функции защиты здесь реализуются на прикладном уровне. Подсистема может быть реализована только при помощи внешних вспомогательных модулей защиты, взаимодействие с которыми осуществляется посредством открытого интерфейса прикладного программирования GSS-APIv2 (Generic Security Services APIv2 — обобщенный прикладной интерфейс программирования для реализации сетевого сервиса безопасности). Интерфейс GSS-API не зависит от конкретной языковой среды и используемых в системе типов криптографических алгоритмов. Это позволяет создавать программные модули, которые на уровне исходного текста не зависят от конкретных механизмов безопасности, применяемых в системе. В качестве внешних модулей могут выступать продукты, основанные на симметричных методах шифрования (например, система аутентификации Kerberos), а также реализующие спецификации X.509 на основе открытых ключей. Совместно с подсистемой SNC обычно используется сервер-шлюз системы — SAProuter, который используется совместно с межсетевым экраном и предназначен для управления сетевыми соединениями, устанавливаемыми с серверами приложений SAP R/3 (рис. 4).

Сервер SAProuter позволяет осуществлять управление сетевыми соединениями на уровне протокола NI (Network Interface), который используется для взаимодействия между компонентами системы. NI-протокол относится к сеансовому уровню модели взаимодействия открытых систем и базируется на стеке TCP/IP. Управление соединениями, установленными через SAProuter,

осуществляется при помощи специальной таблицы маршрутизации, записи которой имеют следующий формат: «<Действие> <Номер порта получателя> <Пароль>». Подсистема аудита предназначена для сбора информации о событиях системы и содержит два типа регистрационных журналов — системный и аудита безопасности. Системный журнал содержит сведения о функционировании ERP-системы, журнал аудита безопасности — данные, связанные с информационной безопасностью системы. Дополнительно подсистема аудита может включать в себя регистрационный журнал сервера SAProuter с данными по всем сетевым соединениям, которые были установлены через этот сервер. Для каждого события подсистема регистрирует дату и время возникновения события, порядковый номер события, категорию события, источник события и другую информацию, связанную с этим событием. Перечень событий, подлежащих аудиту, может быть определен администратором безопасности при помощи фильтров. Фильтры могут содержать следующую информацию: имя пользователя, действия которого должны регистрироваться в журнале аудита; классы событий, регистрируемые системой; уровень приоритета событий, регистрируемых системой, и др. В соответствии с настройками администратора безопасности при возникновении событий определенного типа подсистема аудита безопасности может выводить информацию об этих событиях на консоль администратора системы.

Подсистема аудита, кроме того, должна содержать фильтры, позволяющие фиксировать все события, связанные с действиями пользователя, а также все высокоприоритетные события, касающиеся действий администратора системы.

Контроль идентификации и аутентификации пользователей ERP-системы
Подсистема идентификации и аутентификации предназначена для защиты SAP R/3 от НСД путем проверки аутентификационных данных, предоставляемых пользователями системы. Процедуры идентификации и аутентификации подсистемы могут быть реализованы следующими способами:

- при помощи регистрационных имен и паролей, вводимых пользователями на этапе получения доступа к системе;
- посредством подсистемы SNC, которая была рассмотрена выше;
- с использованием сертификатов X.509. При реализации данного механизма аутентификации вместо регистрационных имен и паролей пользователь предоставляет свой сертификат. Аутентификация с использованием сертификатов X.509 используется при удаленном подключении пользователей к системе через сеть Интернет;
- при помощи механизма SAP Logon ticke» позволяющего реализовать единую процедуру регистрации в системе — Single Sign On (SSO).

При использовании первого способа аутентификации возникает реальная угроза получения несанкционированного доступа к системе путем подбора пароля. Для минимизации такого риска необходимо выполнить ряд превентивных мер, описание которых приведено ниже.

Ограничение числа попыток доступа к системе. Для выполнения этого действия необходимо внести дополнительные параметры в профиль системы путем выполнения транзакции RZ10 или ручного редактирования файла, содержащего профиль.

Настройка правил по формированию и смене пароля. Для выполнения настройки вначале указывается минимально допустимая длина пароля и время, необходимое для смены пароля. Кроме изменения профиля администратор безопасности должен определить перечень паролей, использование которых пользователями в системе SAP R/3 является недопустимым.

Помимо встроенных правил формирования паролей администратор безопасности должен учитывать следующие требования к парольной защите:

• пароль не должен совпадать с именем учетной записи пользователя;
• пароль должен содержать алфавитные символы разных регистров;
• пароль должен содержать как алфавитные, так и цифровые символы;
• пароль должен представлять собой случайную последовательность символов.

Необходимо отметить, что в целях безопасности в системе SAP R/3, как и во многих других, хранятся не пароли пользователей, а их хэш-значения. Для их вычисления используется модифицированный алгоритм MD5. Настройка параметров защиты стандартных пользователей. В процессе установки системы SAP R/3 создаются несколько встроенных учетных записей с паролями, заданными по умолчанию. В дополнение к рассмотренным выше подсистемам для защиты SAP R/3 применяются штатные средства, встроенные в операционные системы (ОС) и системы управления базой данных (СУБД), на основе которых разворачивается SAP R/3.

Представленный анализ уровня защищенности ERP-систем на примере SAP R/3 внушает определенный оптимизм производителям и пользователям. Однако все базовые подсистемы защиты SAP R/3 предполагают применение внешних модулей, реализующих криптографические функции в соответствии с заданными требованиями. В настоящее время присутствует несколько таких модулей, но все они реализуют зарубежные криптографические алгоритмы, что усложняет их использование на территории России. Кроме того, подсистемы защиты, встроенные в SAP R/3, имеют целый ряд недостатков. Например, подсистема идентификации и аутентификации применяет регистрово-независимые пароли; функции защиты подсистемы SNC реализуются на прикладном уровне, а трафик сетевого и транспортного уровней передается по сети в незащищенном виде; сервер SAProuter не имеет функций идентификации пользователей, инициировавших соединение через сервер, и др.

Необходимо также отметить, что подсистемы защиты, входящие в состав SAP R/3, обеспечивают решение узкого круга задач информационной безопасности, касающихся защищенных сетевых соединений и криптографической защиты электронных документов. Функции противодействия остальным угрозам безопасности, реализуемым в виде сетевых атак, несанкционированный доступ к компонентам системы с консоли управления и др., возлагаются на внешние специализированные комплексы защиты.

Для того чтобы программный продукт был пригоден для использовании в России, необходимо чтобы он прошел соответствующую сертификацию. Для программных продуктов существуют требования к показателям защищенности. Существуют семь уровней защищенности. Для программных комплексов экономического класса, коим и является система SAP R/3, достаточно чтобы они соответствовали требованиям к показателям четвертого класса защищенности. Опишем основные требования к показателям четвертого класса защищенности:

- Дискреционный принцип контроля доступа
- Мандатный принцип контроля доступа
- Очистка памяти
- Изоляция модулей
- Маркировка документов
- Защита ввода и вывода на отчуждаемый физический носитель информации
- Сопоставление пользователя с устройством
- Идентификация и аутентификация

Исходя из вышеперечисленных требований можно заключить что система SAP R/3 вполне удовлетворяет этим требованиям только после некоторой доработки используемых подсистем

защиты. Самой большой доработкой является адаптирование внешних модулей для использования в них криптографических функций, основанных на отечественных ГОСТах.

Анализируя недостатки SAP R/3, можно заметить, что для более безопасного применения этой системы необходимо изменить систему аутентификации, добавить в модуль SNC алгоритм шифрования трафика сетевого и транспортного уровней, оснастить SAProuter системой идентификации пользователей, инициировавших соединение через сервер. Существенной доработки требует внешняя система безопасности, однако, для российского рынка она может быть вообще заменена на отечественный аналог, в большей степени соответствующий ГОСТам (таким аналогом может выступить система «Кобра» или «Страж»). Несмотря на ориентацию системы SAP R/3 на западный рынок, специалисты отдела разработок делают небезуспешные попытки адаптирования некоторых модулей, входящих в состав системы, под Российский рынок. Так, например, в испытательной лаборатории компании «Микротест» (Россия) завершились сертификационные испытания базисной системы для разработки прикладного программного обеспечения со встроенными средствами защиты от несанкционированного доступа SAP Basis system release 4.6X, входящей в состав комплексного продукта SAP R/3. По результатам сертификационных испытаний и согласно требованиям руководящего документа Гостехкомиссии России базисная система SAP Basis system release 4.6X соответствует четвертому классу защищенности и может быть использована для разработки прикладного программного обеспечения автоматизированных систем до класса защищенности 1В включительно. В настоящее время сертификационные испытания в лаборатории «Микротест» проходят прикладные компоненты mySAP.com. В недавнее время компания "Микротест" объявила об успешном завершении работ по сертификации интегрированной системы управления предприятием SAP R/3. Впервые в России крупная корпоративная система стандарта ERP (Enterprise Resource Planning) была сертифицирована Гостехкомиссией при Президенте РФ. После испытаний, проведенных лабораторией безопасности информации компании "Микротест", Гостехкомиссия выдала сертификат № 306, подтверждающий, что система SAP R/3 версии 4.0В является защищенным программным средством обработки информации со встроенными средствами защиты от несанкционированного доступа. Сертификат удостоверяет, что система SAP R/3 соответствует требованиям руководящего документа Гостехкомиссии "Средства вычислительной техники. Защита от несанкционированного доступа к информации" по 4 классу защищенности. Система SAP R/3, призванная обеспечить интеграцию финансово-хозяйственной деятельности крупнейших предприятий России, была установлена на платформе Solaris 2.6 под управлением СУБД Oracle 8.0.5.

Все результаты тестирования можно посмотреть в сертификате № 306, выданном Гостехкомиссией при Президенте РФ.

В настоящее время на многих организациях введены в эксплуатацию модули системы SAP R/3. Ниже приведен список организаций и модулей, работающих на этих предприятиях.

ОАО "Омский НПЗ"
Система финансового учета и отчетности "Омского НПЗ" на базе модулей FI, CO системы SAP R/3.

ОАО "Славнефть-Ярославнефтеоргсинез"
Единая информационно-управляющая система "Славнефть-Ярославнефтеоргсинез" на базе модулей FI, FI-AA, CO, MM, SD системы R/3.

ОАО "Омскгоргаз"
Система финансового учета и отчетности (функциональность модулей FI, CO системы R/3).

ООО "Сургутгазпром"
Интегрированная автоматизированная система управления (функциональность модулей FI, CO системы R/3). Первый этап.

Литература:

1. Administering SAP R/3 The Fi - Financial Accounting and CO - Controlling Modules
2. SAP R/3 системное администрирование. Вилл Л.
3. Разработка приложений для SAP R/3 на языке ABAP/4. Р.Кречмер, В.Вайс
4. The Sap R/3 Handbook. Jose Antonio Hernandez
5. www.korn.ru