системы. Необходимость данных действий вызвана тем, что приведенный подход основан на подсчете неизвестных в системе, а когда существует избыточность членов уравнений, то она влияет на количество неизвестных в системе, но не влияет на общую зависимость в структуре системы. Чтобы минимизировать этот недостаток необходимо провести процедуру нормализации системы, которая заключается в суммировании по модулю два уравнений системы. Также существует второстепенные преобразования, относительно которых выработаны рекомендации по их использованию.

Анализ приведенного подхода показывает, что его вычислительная сложность ниже экспоненциальной, так как самая трудоемкая часть алгоритма (нормализация системы) имеет максимальное количество операций, которое равно сочетанию из $N/2$ по 2, где N – разрядность числа, подлежащего факторизации.

III Заключение

В настоящее время еще нельзя утверждать, что приведенный подход является алгоритмом в том смысле, что известны конкретные действия для любой комбинации значений разрядов в сомножителях. Но уже понятно, что на основе данного подхода может быть организована атака на ассиметричные криптосистемы, сложность реализации которой может быть ниже экспоненциальной. В настоящее время ведется дальнейшая работа по развитию данного подхода, а также всех процедур, в него входящих.

*Литература: **1**. Шнайер Б. Прикладная криптография. – М.: Издательство ТРИУМФ, 2003 – 816 с.: ил. **2**. Жилин А. В., Мохор В. В. Структурный метод факторизации больших целых чисел// Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України, спец. випуск - К.: 2008. - С. 49 – 57.*

УДК 004.4

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ERP-СИСТЕМАХ

Александр Голяка
Национальный банк Украины

Аннотация: **В работе рассматривается проблема защиты информации в ERP-системах, возможности ее решения с помощью внутренних механизмов систем на примере SAP R/3. Показана необходимость создания внешних криптографических библиотек защиты обязательно реализованных с использованием интерфейсов SSF и GSS API, которые открыты для внешних разработчиков в системах SAP. Описаны принципы работы функций SSF-API, форматы входных/выходных данных.**
Summary: **The defense of information in ERP-sistems is considered.**
Ключевые слова: **Защита информации в ERP-системах, форматы входных – выходных данных.**

Системы класса ERP – (Enterprise Resource Planning – Планирование Ресурсов Предприятия) – это комплекс интегрированных приложений, позволяющих создать единую среду для автоматизации планирования, учета, контроля и анализа всех основных бизнес-процессов предприятия. Такие системы предполагают управление всеми (или отдельными) ресурсами предприятия – трудовыми, финансовыми, материальными и пр. Как правило, ERP-система состоит из набора подсистем, таких как: финансы, снабжение и сбыт, хранение, производство и пр. Одной из наиболее совершенных и типичных представителей класса ERP-систем, являющаяся, по сути, отраслевым стандартом в этой области, является система SAP R/3, разработанная немецкой компанией SAP AG.

Система SAP R/3 основана на трехзвенной архитектуре. С точки зрения SAP R/3, трехзвенная архитектура состоит из презентационного уровня, уровня приложений и уровня базы данных (БД) (рис. 1).

С точки зрения аппаратных средств эти уровни независимо функционируют на разных компьютерах или совместно на одном в зависимости от конфигурации системы (одноуровневая/двухуровневая/трехуровневая). Кроме того, SAP R/3 позволяет распределять презентационный уровень и уровень приложений по нескольким компьютерам.

Для больших предприятий с точки зрения производительности наиболее эффективна трехуровневая конфигурация. В такой конфигурации несколько разных серверов приложений могут одновременно обрабатывать данные, хранящиеся на общем сервере БД.

Фактические вычисления и оценки системы выполняются на серверах приложений. Уровень БД представляет собой реляционную систему управления базой данных (РСУБД). Обмен данными между РСУБД и процессами приложений осуществляется через интерфейс SQL. Презентационный уровень

представляет собой графический пользовательский интерфейс SapGui (Graphical User Interface), через который происходит обмен информацией между пользователем и уровнем приложений.

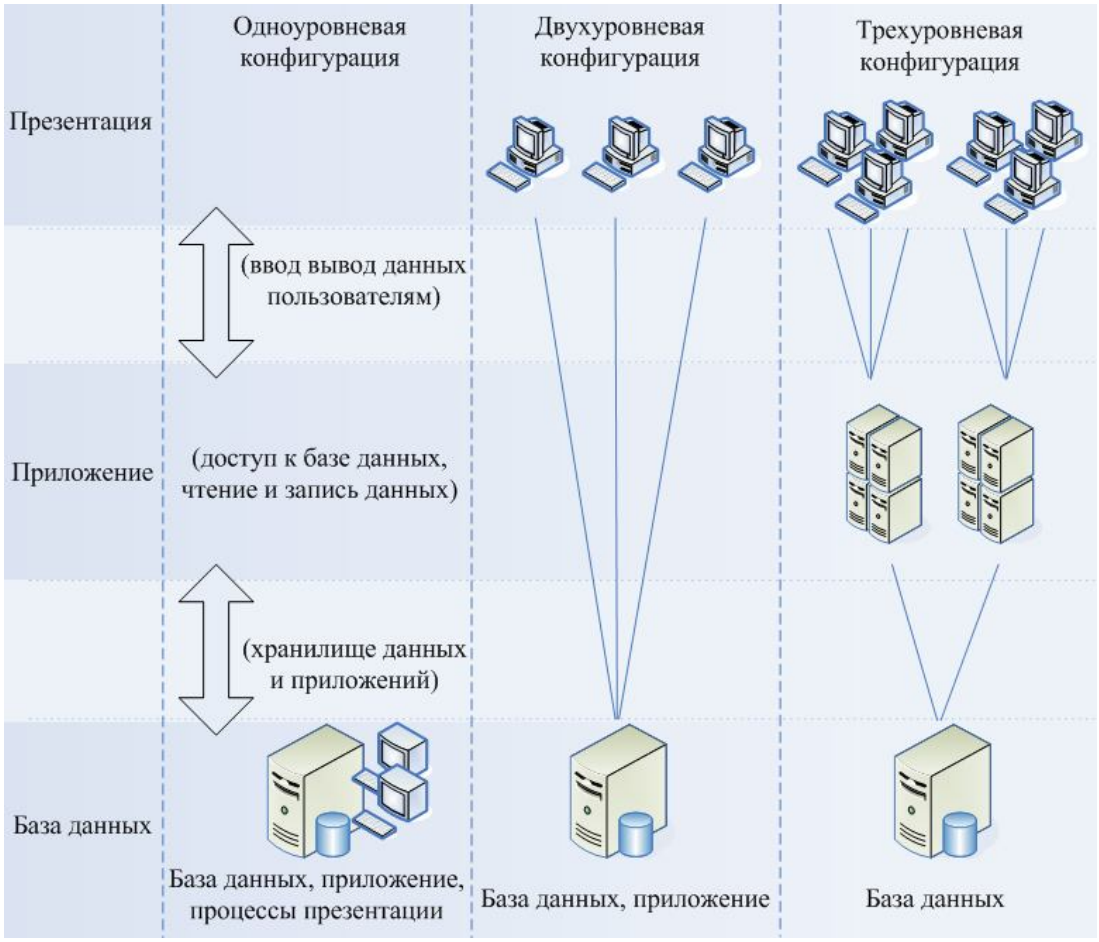

Рисунок 1 – Трехзвенная архитектура SAP R/3

Для взаимодействия уровней, распределенных по нескольким компьютерным системам, используется протокол TCP/IP. Для взаимодействия компьютеров презентационного уровня и серверов приложений обычно используются соединения глобальной сети, серверы БД следует соединять с помощью локальной сети. Система SAP R/3 соединяется с Internet через сервер транзакций (ITS, Internet Transaction Server). ITS состоит из двух программных компонентов: процесса A-шлюза (application gate – шлюз приложения) и процесса W-шлюза (Web gate – шлюз Web). Процесс A-шлюза устанавливает соединение с сервером приложения SAP R/3, а процесс W-шлюза – с Web-сервером. Оба компонента взаимодействуют друг с другом по протоколу TCP/IP. Сервер ITS преобразует запросы из WWW в запросы, сформулированные согласно стандарту SAPGUI. Для этого используется протокол DIAC (Dynamic Information and Action Gateway), а также ISAPI (Microsoft Information Server API) и NSAPI (Netscape Server API), являющиеся интерфейсами прикладного программирования. ITS позволяет выполнять прикладные компоненты Internet (IAC, Internet Application Components).

В связи с описанной архитектурой SAP R/3, можно сформулировать базовый перечень характерных программно-технических угроз (без учета техногенных и пр. угроз), которым могут подвергаться ERP-системы в общем случае:

1. Нарушение конфиденциальности данных, передаваемых между компонентами ERP-системы.
2. Несанкционированное искажение данных, передаваемых между компонентами ERP-системы.
3. Получение несанкционированного доступа (НСД) к информации, хранимой в БД ERP-системы.
4. Нарушение целостности данных, хранимых в БД ERP-системы.
5. Отказ одного из субъектов ERP-системы от совершенных им действий по отправке или получению информации, или утверждение, что информация отправлена/получена в другое время.

6. Навязывание субъектам ERP-системы неверной информации, в т. ч. служебной.
7. Маскировка под зарегистрированного пользователя (или запросы) системы.
8. Нарушение работоспособности серверов ERP-системы.
9. Группа угроз технической инфраструктуры ERP-системы.
10. Типовые угрозы информационно-телекоммуникационных систем.

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

1. Информация, передаваемая между компонентами ERP-системы.
2. Информация, хранимая в БД ERP-системы.
3. Сервера ERP-системы.

Методы и средства обеспечения информационной безопасности

Система SAP R/3 содержит встроенный комплекс средств защиты информации, состоящий из четырех подсистем: SSF (Secure Store & Forward), защиты сетевых соединений SNC (Secure Network Communication), аудита (Audit Information System), идентификации и аутентификации.

Подсистема SSF предназначена для обеспечения защиты электронных документов ERP-системы. 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). Конкретные криптографические алгоритмы механизмов не регламентированы, а вот форматы данных, используемые подсистемой SSF в процессе формирования цифровых подписей и конвертов, должны соответствовать стандарту PKCS#7. В расширенной комплектации SAP R/3 предусмотрена подсистема SSF, реализованная при помощи вспомогательной библиотеки SAPSECULIB (SAP Security Library), которая, в связи с экспортными ограничениями страны разработчика на средства защиты информации и криптостойкость, использует нестойкие криптографические функции для защиты информации и не поддерживает механизм цифровых конвертов. В связи с этим для реализации полнофункциональной подсистемы SSF необходимо (и такая возможность есть) 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. Для взаимообмена открытыми ключами между пользователями системы могут быть задействованы удостоверяющие центры (Certification Authority), которые обеспечивают распределение сертификатов, содержащих открытые ключи пользователей системы. Сертификаты, распределяемые удостоверяющим центром, подписываются электронной подписью этого центра. Формат сертификата должен соответствовать рекомендациям X.509v3.

Архитектура подсистемы SSF изображена на рис. 2.

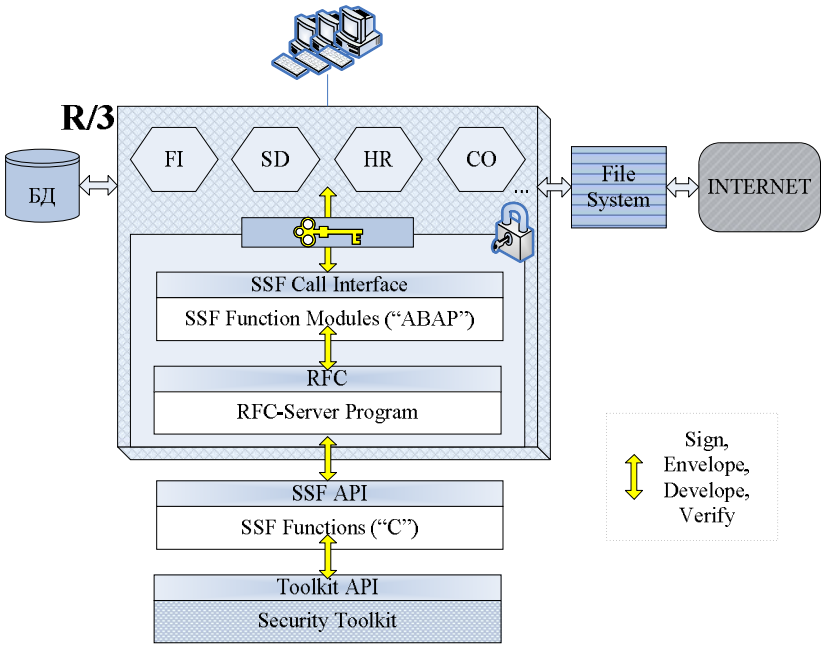

Рисунок 2 – Архитектура SSF

Приложения (FI, SD, и т. п.) SAP R/3 обращаются к функциям SSF, используя различные функциональные модули ABAP с помощью интерфейса вызова SSF базисного программного обеспечения. Соответствующий SSF ABAP функциональный модуль в свою очередь обращается к необходимым функциям “C” (функциям подписи, шифрования и т. д.) через так называемый модуль RFC (“Remote Function Call”) SAP R/3. SSF RFC серверный модуль или ядро SAP R/3 обращаются к функциям “C” используя интерфейс SSF-API. В завершение цепочки обращений, библиотека SSF-API функций динамически загружает выбранную для защиты информации внешнюю криптографическую библиотеку (“security toolkit”) или содержит в себе конкретные реализации механизмов криптографической защиты. Библиотека криптографической защиты, запрограммированная с учетом интерфейса SSF-API, будет гарантированно понятна SAP R/3 и может быть встроена в эту систему.

Схема работы электронной цифровой подписи SSF показана на рис. 3.

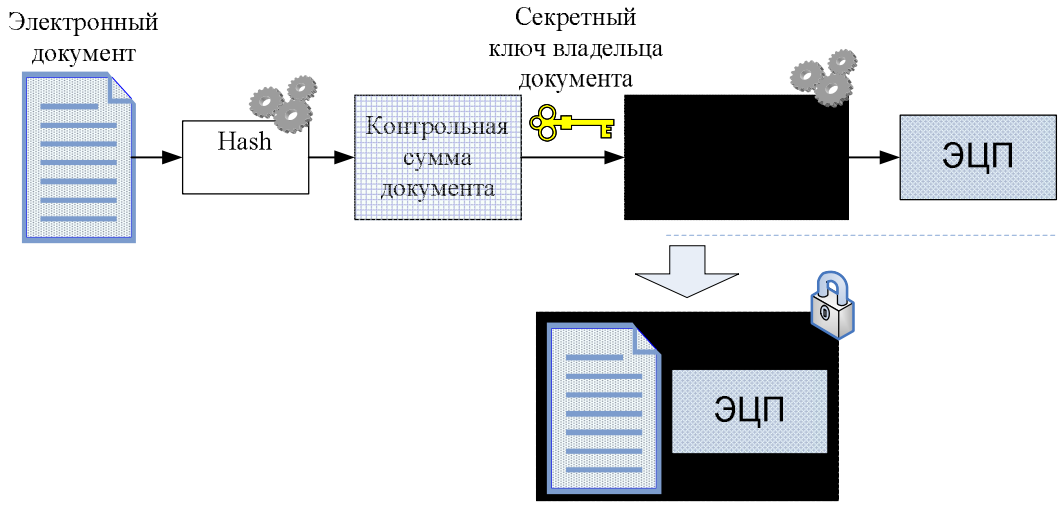

Рисунок 3 – Схема формирования электронной цифровой подписи

На рисунке изображен процесс подписи электронного документа, проверка подписи происходит в обратном порядке. Схема работы электронного цифрового конверта показана на рис. 4.

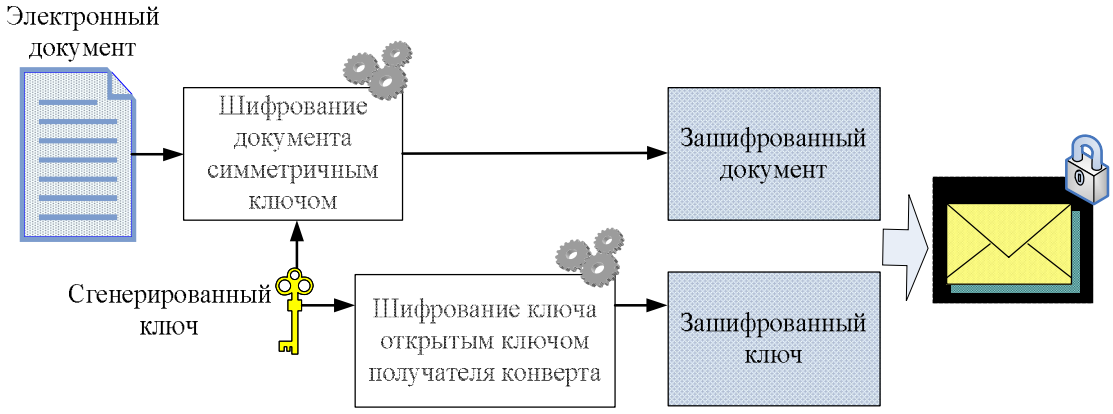

Рисунок 4 – Схема формирования электронного цифрового конверта

На рисунке изображен процесс шифрования, процесс расшифровки происходит в обратном порядке.

Созданные таким образом цифровые конверты можно отправлять за пределы инфраструктуры SAP R/3, хранить в БД, передавать другим пользователям SAP R/3 и т. д., электронные документы в них защищены.

Форматы данных, используемые SSF-API:

1. DATA для вложения входных данных.

2. SIGNED DATA для инкапсуляции подписанной информации.
3. ENVELOPED DATA для инкапсуляции зашифрованных данных.
4. DIGESTED DATA для инкапсуляции хэшированных данных.

Типы данных, используемые для формирования защищенных конвертов описываются с помощью абстрактного синтаксиса нотаций ASN.1.

Структура конверта SIGNED DATA изображена на рис. 5.

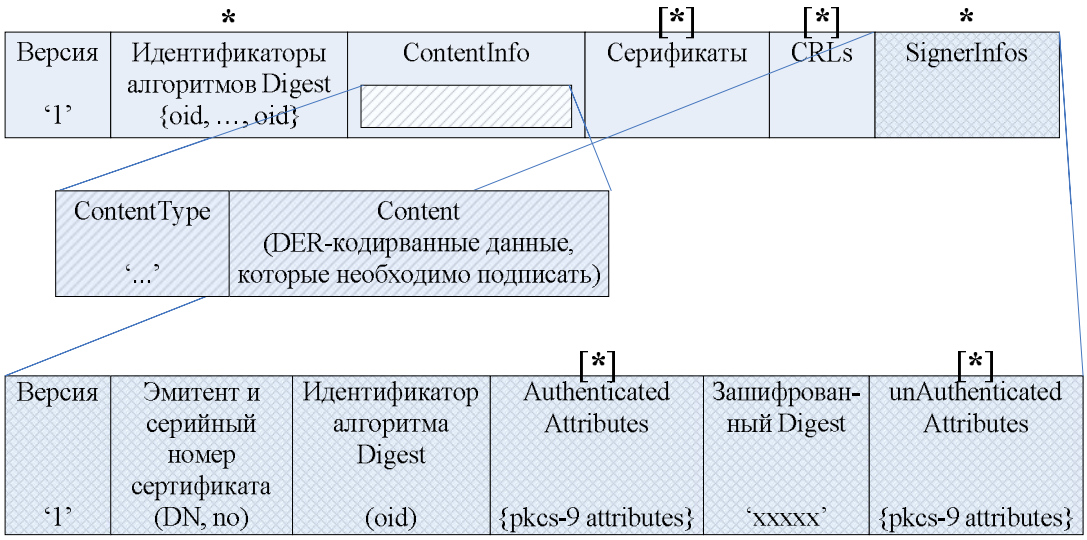

Рисунок 5 – Структура конверта SIGNED DATA

В соответствии со спецификацией PKCS #7, для формирования конверта SIGNED DATA используется тип данных SignedData, описываемый следующим образом:

SignedData ::= SEQUENCE {
version Version,
digestAlgorithms **DigestAlgorithmIdentifiers**,
contentInfo ContentInfo,
certificates,
signerInfos **SignerInfos**
}
DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier
SignerInfos ::= SET OF **SignerInfo**
SignerInfo ::= SEQUENCE {
version Version,
issuerAndSerialNumber IssuerAndSerialNumber,
digestAlgorithm DigestAlgorithmIdentifier,
authenticatedAttributes
[0] IMPLICIT Attributes OPTIONAL,
digestEncryptionAlgorithm
DigestEncryptionAlgorithmIdentifier,
encryptedDigest **EncryptedDigest**,
unauthenticatedAttributes
[1] IMPLICIT Attributes OPTIONAL
}
EncryptedDigest ::= OCTET STRING

Структура конверта ENVELOPED DATA изображена на рис. 6.

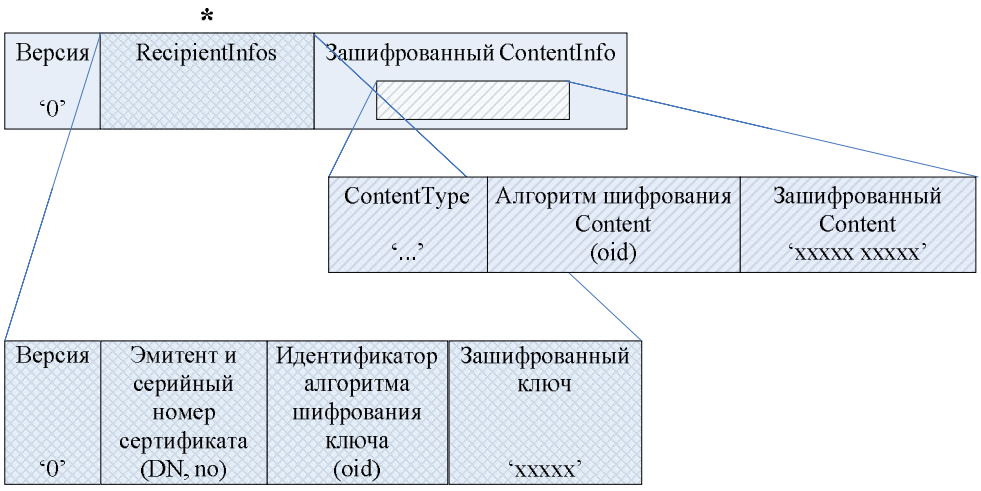

Рисунок 6 – Структура конверта ENVELOPED DATA

В соответствии со спецификацией PKCS #7, для формирования конверта ENVELOPED DATA используется тип данных EnvelopedData. Описывается он так:

……

EnvelopedData ::= SEQUENCE {
version Version,
recipientInfos **RecipientInfos**,
encryptedContentInfo **EncryptedContentInfo**
}
RecipientInfos ::= SET OF **RecipientInfo**
RecipientInfo ::= SEQUENCE {
version Version,
issuerAndSerialNumber IssuerAndSerialNumber,
keyEncryptionAlgorithm
KeyEncryptionAlgorithmIdentifier,
encryptedKey **EncryptedKey**
}
EncryptedKey ::= OCTET STRING
EncryptedContentInfo ::= SEQUENCE {
contentType ContentType,
contentEncryptionAlgorithm
ContentEncryptionAlgorithmIdentifier,
encryptedContent
[0] IMPLICIT **EncryptedContent** OPTIONAL
}
EncryptedContent ::= OCTET STRING

……

Структура конверта DIGESTED DATA изображена на рис. 7.

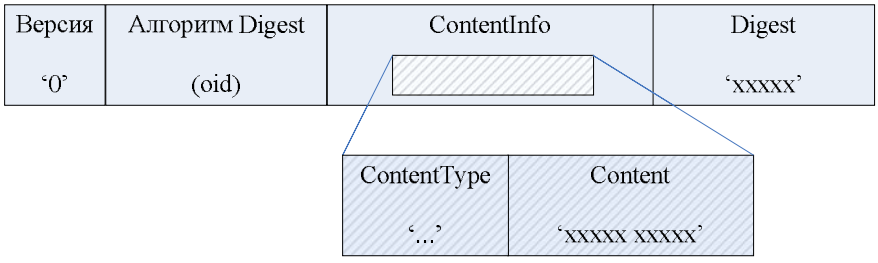

Рисунок 7 – Структура конверта DIGESTED DATA

Во всех конвертах SSF применяется поднабор правил кодирования DER (Distinguished Encoding Rules, описаны в стандарте X.509), которые определяют однозначные способы кодирования перечисленных типов.

Основные интерфейсные функции SSF-API:

1. SsfVersion – возвращает информацию о текущей версии библиотеки SSF-API и программного продукта, обеспечивающего криптографическую защиту.
2. SsfQueryProperties – определяет свойства механизмов защиты, которые могут быть применены библиотекой.
3. SsfEncode – преобразовывает входной текст в форму закодированного формата. В соответствии с PKCS#7 это функция ASN.1 кодирования, т. е. преобразования данных в бинарный формат (Octetstring) для возможности передачи между различными операционными системами. В PKCS#7 для этого используется формат «Data». Данные при этом не защищаются цифровой подписью или шифрованием.
4. SsfDecode – Octetstring закодированный SsfEncode, с помощью этой функции декодируется в исходный формат данных. В SSF-API практически каждая функция имеет парную, осуществляющую преобразование данных в предыдущее состояние.
5. SsfSign – генерирует одну или более цифровых подписей на основании входного буфера данных.
6. SsfAddSign – добавляет дополнительную подпись к данным в цифровом конверте, сформированном функцией SsfSign.
7. SsfVerify – используется для проверки цифровой подписи. Эта функция парная для SsfSign.
8. SsfEnvelope – шифрует данные для каждого получателя в указанном списке.
9. SsfDevelope – расшифровывает данные, зашифрованные SsfEnvelope (функция парна SsfEnvelope).
10. SsfDigest – используется для подсчета хеш значения входных данных.
11. SsfDELSsfOctetstring – удаляет возвращаемые другими SSF-API функциями данные, и освобождает занимаемую ими память.

Группа вспомогательных функций работает со структурой данных (создают, удаляют структуры, элементы структур), содержащей информацию о сертификате, пути к секретному ключу, идентификаторе пользователя и т. д., а также со списком таких структур (данные функции можно запрограммировать при помощи связанных списков). Несколько функций отвечают за отображение структур, содержащих информацию о пользователях, и списков таких структур.

Функции безопасного хранения и передачи данных SSF-API могут применяться в различных сценариях для защиты данных и документов. К типичным сценариям в решениях SAP относятся следующие:

1. Приложение, использующее механизмы SSF, преобразует незашифрованные данные из презентационного уровня – графического пользовательского интерфейса SAP (SapGui – Graphical User Interface), в защищенный формат и сохраняет их в базе данных используемого решения SAP. При последующих обращениях приложения к этим данным они извлекаются из базы данных и дешифруются с использованием функций SSF-API. Если данные подписаны электронной подписью, приложение может также проверить электронную подпись.
2. Приложение считывает данные из базы данных SAP и подготавливает их для внешней передачи или сохранения. Для этого данные сначала преобразуются в соответствующий внешний формат, затем защищаются с использованием функций SSF-API. После преобразования данных в защищенный формат приложение может безопасно сохранять их на носителе данных (например, на диске или в архиве данных) или передавать их по (возможно) незащищенным каналам связи (таким как Internet). Санкционированным получателем может быть другое приложение SAP или другая система, поддерживающая используемый защищенный формат SSF-API.
3. Приложение получает защищенные данные или данные, подписанные электронной подписью, из внешнего источника и импортирует их в приложения SAP. Если данные защищены с использованием формата, совместимого с SSF-API, то приложение может использовать функции SSF-API для расшифровки данных или проверки подписи.

Подсистема SNC является дополнительным опциональным программным модулем в SAP R/3 и предназначена для организации защищенных сетевых соединений, которые устанавливаются между распределенными компонентами системы. SNC позволяет осуществлять аутентификацию субъектов, устанавливающих соединение, а также обеспечивать конфиденциальность и целостность данных, передаваемых в рамках установленного соединения. Все функции защиты реализуются, аналогично SSF, 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 также не

зависит от конкретной языковой среды и используемых в системе типов криптографических алгоритмов, что позволяет создавать программные модули, которые на уровне исходного текста не зависят от конкретных механизмов безопасности, применяемых в системе. Тем самым реализуется открытость прикладных систем и соответствующих средств защиты. 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.

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. 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 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:

1. при помощи регистрационных имен и паролей, вводимых пользователями на этапе получения доступа к системе;
2. посредством подсистемы SNC;
3. 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 в основном используется при удаленном подключении пользователей к системе через сеть Internet;
4. при помощи механизма SAP Logon ticket позволяющего реализовать единую процедуру регистрации в системе.

В заключение можно подчеркнуть, что SAP R/3 должны быть оснащены модулями защиты с криптографическими функциями, основанными на отечественных стандартах. Кроме того, функциональные возможности системы безопасности (SSF, SNC) должны быть дополнены специализированными средствами защиты (например, межсетевыми экранами, системами обнаружения атак, активного мониторинга, антивирусными системами и др.). Лишь при решении этих задач информационная безопасность SAP R/3 и других ERP-систем данного класса будет соответствовать требованиям, предъявляемым к системам защиты.

Литература: ***1.*** *PKCS #7: Cryptographic Message Syntax Standard* ***2.*** *J. Linn. RFC 1421: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. February 1993.* ***3.*** *НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. Утверджено приказом ДСТСЗИ СБ Украины от 08.11.2005 №125.* ***4.*** *НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Утверджено приказом ДСТСЗИ СБ Украины от 28.04.1999 №22.*

УДК 004.056.5 (076.5)

МЕХАНІЗМ КОДУВАННЯ ТА ОБРОБКИ ІНФОРМАЦІЇ В СИСТЕМАХ ІЗ ХАОСОМ

Богдан Корнієнко, Олександр Неділько
Національний авіаційний університет

Анотація: **В комунікаційних системах хаос може використовуватися як носій інформації і як динамічний процес, що забезпечує перетворення інформації до нового вигляду. Методи хаотичного кодування є зручним засобом організації віртуальних корпоративних мереж із забезпеченням заданого рівня конфіденційності інформації. В статті досліджується можливість використання хаосу для обробки інформації, розглядається модель хаотичного процесора.**