УДК 004.056

С.В. Запечников

Архитектура и алгоритмическое обеспечение системы криптографической обработки информации, стойкой к частичному разрушению ключей

Представлена архитектурная модель и концепция реализации универсальной системы криптографической защиты информации, предназначенной для функционирования в распределенных компьютерных средах. Предложена обобщенная структурно-функциональная модель системы. Обсуждаются требования к аппаратному, программному обеспечению системы и управлению ключами.

Ключевые слова: распределенные компьютерные системы, живучесть, защита информации, криптография, управление ключами.

Введение

Существующие средства защиты информации (СЗИ) характеризуются слабыми показателями живучести в условиях частичного разрушения распределенных компьютерных систем (РКС), в которых они функционируют. Проведенный автором анализ зарубежных разработок в области создания СЗИ, сохраняющих стойкость при воздействии на РКС комплекса дестабилизирующих факторов различной природы, подтвердил актуальность решения этой проблемы, но в то же время выявил ряд проблем. Основные недостатки существующих СЗИ заключаются в следующем:

- отсутствуют комплексные решения по защите функциональных и информационных ресурсов РКС и прикладных программ (ПП), что не позволяет строить на их основе защищенные информационные системы;
- существующие системы в основном ориентированы на локальные или малые РКС, предоставляют очень ограниченный набор функций;
- отсутствуют средства автоматического восстановления системы после атак противника.

Составной частью обозначенной проблемы является задача обеспечения стойкости СЗИ к разрушению и компрометации части криптографических ключей или ключевой системы в целом. Современные средства криптографической защиты информации характеризуются высокой стойкостью применяемых в них криптографических алгоритмов, поэтому нарушение их безопасности посредством криптоаналитических атак маловероятно. Похищение или разрушение ключей может быть значительно проще для противника, а по эффективности сопоставимо с криптоанализом.

1. Требования к системе криптографической обработки информации

В результате оценки существующих решений и основываясь на доказанных автором ранее теоретических результатах [1] определена система требований к методам и алгоритмам системы криптографической обработки информации (СКОИ), сохраняющей стойкость в условиях разрушительных воздействий.

1. СКОИ должна соответствовать общепринятым концепциям построения открытых информационных систем (обеспечивать переносимость, способность к взаимодействию, масштабируемость, управляемость), а также международным стандартам по распределенной обработке данных и моделям защиты информации, российским стандартам по криптографическим методам защиты информации.
2. СКОИ должна функционировать в условиях корпоративной информационной системы, т.е. при наличии единой иерархической схемы управления системой, должна обеспечивать достаточные возможности управления защитой, контроля и учета использования ресурсов, требовать минимального количества «ручных» операций по обслуживанию и настройке.

3. СКОИ должна предоставлять возможно более полный набор типовых средств и механизмов криптографической защиты.
4. СКОИ должна учитывать реальные модели действующего в системе противника, а также вычислительные и коммуникационные возможности участников РКС. Архитектура СКОИ должна позволять настраивать ее функции, адаптируя к тому или иному типу противника, например, пассивному, активному.
5. СКОИ должна обеспечивать стойкость каждой отдельно взятой подсистемы (сервиса защиты) в условиях разрушения некоторого, заранее определенного, количества криптографических ключей.

Обобщающий термин «*разрушение ключевого материала*» будем использовать для обозначения утраты одного или более свойств, которыми характеризуется безопасность ключевого материала: доступности, аутентичности и (или) секретности.

Реализовать перечисленные требования на базе отечественных стандартов криптографической защиты позволяют разработанные ранее алгоритмы и протоколы: способ защищенной рассылки сообщений в РКС [2], пороговые схемы цифровой подписи на основе ГОСТ Р 34.10-2001 [3, 4] и метод безопасного размещения информационных массивов в РКС [5].

2. Структурно-функциональная модель системы

Первым шагом по пути создания СКОИ, сохраняющей стойкость в условиях разрушительных воздействий, является разработка ее структурно-функциональной модели. Модель строилась при следующих предположениях: СКОИ функционирует в среде корпоративной информационной системы на базе РКС из множества серверов, обслуживающих клиентские системы (рабочие станции, персональные компьютеры и терминалы). Все они связаны между собой транспортной коммуникационной инфраструктурой. Кроме того, РКС может быть связана с внешней глобальной средой Интернет. Точная конфигурация коммуникационной инфраструктуры не рассматривается, но предполагается, что в отсутствии отказов каждый узел РКС может передавать данные любому другому узлу за ограниченный промежуток времени. Концептуально СКОИ представляется как комплекс программ «промежуточного слоя» (middleware), расширяющих функции операционных систем узлов РКС и формирующий для ПП защищенную среду передачи, хранения и обработки данных посредством предоставления определенных услуг – сервисов, доступных через интерфейс прикладного программирования (ИПП).

Логическая организация СКОИ в целом включает два уровня.

1. *Нижний уровень («уровень защиты распределенной среды»)* формирует защищенную среду хранения и передачи данных между узлами РКС, которая обеспечивает:
   - реализацию для множества системных ключей СКОИ выбранных для них схем управления ключевым материалом, обеспечивающих заданные администратором системы показатели доступности;
   - контроль доступа субъектов системы к ключевому материалу, хранящемуся на узлах РКС;
   - аутентичность и, если необходимо, секретность ключевого материала, размещаемого в РКС;
   - организацию каналов защищенной связи, т.е. гарантии аутентичности и, если необходимо, секретности передаваемых по коммуникационным каналам сообщений в условиях компрометации противником части узлов РКС (для нескомпрометированных участников);
   - автоматическое восстановление скомпрометированных узлов РКС либо оповещение оператора системы при невозможности этого.
2. *Верхний уровень («уровень поддержки ПП»)* реализует различные функции защиты информации, которые предоставляются ПП в виде услуг, доступных им через ИПП. Верхний уровень, в свою очередь, пользуется услугами нижнего уровня через определенный интерфейс. Примерный состав сервисов, которые СКОИ должна предоставлять ПП в виде функций ИПП, предполагается таким:

- удостоверение открытых ключей ПП в криптосистемах с инфраструктурой открытых ключей и сопутствующие услуги;
- генерация секретных ключей и частичных секретных ключей ПП в идентификационных и бессертификатных криптосистемах;
- трансляция секретных ключей ПП;
- распределение секретных ключей ПП;
- распределение ключей конференц-связи;
- распределенная генерация цифровой подписи;
- нотариальное заверение сообщений, поставляемых ПП;
- хранение секретных данных, поставляемых ПП;
- защищенная пересылка сообщений ПП;
- генерация псевдослучайных чисел.

Набор базовых функций позволит реализовать на их основе широкий спектр средств защиты, расширяя и наращивая функциональность СКОИ.

Физическая организация СКОИ. СКОИ составляется из множества взаимодействующих аппаратно-программных комплексов на серверах РКС, каждый из которых содержит программное обеспечение СКОИ совершенно одинакового состава и структуры, что обеспечивает максимальную живучесть системы. Такой подход позволяет создать аппаратно-программную платформу для реализации многочисленных средств и механизмов криптографической защиты для ПП в среде, подверженной воздействию дестабилизирующих факторов.

Определение общих принципов логической и физической организации СКОИ позволяет конкретизировать пути и способы реализации такой системы, а именно: спроектировать архитектуру ПО, сконструировать алгоритмическое и протокольное обеспечение, дать рекомендации по составу программного, аппаратного и информационного обеспечения СКОИ.

3. Основные элементы реализации системы

Архитектура СКОИ. Архитектура ПО, размещаемого на каждом узле СКОИ, является многоуровневой. На рисунке 1 показаны основные архитектурные компоненты СКОИ во взаимосвязи с другим системным ПО.

Центральным элементом архитектуры является ядро СКОИ, управляющее процессами. Все остальные подсистемы СКОИ, выполняющие функции защиты, организованы в многоуровневую схему. Самый нижний уровень – подсистема контроля доступа при выполнении операций чтения/записи физических блоков данных; следующий – подсистемы, реализующие «уровень защиты распределенной среды»; верхний составляют подсистемы, реализующие «уровень поддержки ПП». Функции последних заключаются в предоставлении ПП тех или иных услуг, которые доступны через ИПП СКОИ. Сервисы нижних уровней доступны подсистемам верхних уровней через интерфейсы, которые должны быть специфицированы при реализации СКОИ. В свою очередь, подсистемы нижнего уровня для выполнения своих функций пользуются сервисами ядра СКОИ и ОС.

Алгоритмическое и протокольное обеспечение СКОИ реализует принцип систем с дробной кратностью резервирования, в том числе пороговые криптосхемы, и модель «активной безопасности» [6]. Оно полностью соответствует структурно-функциональной модели и включает в себя криптографические протоколы для 22 подсистем СКОИ. Его структура обусловлена архитектурой СКОИ и состоит из ряда взаимосвязанных модулей, реализующих подсистемы СКОИ, как показано на рисунке 2.

Информационное обеспечение СКОИ. Каждый узел РКС должен содержать минимальный набор данных, необходимых для обеспечения работы системы: данные о конфигурации и настройках, сетевые адреса узлов, идентификаторы криптографических алгоритмов, исходные персональные ключи. Все данные, за исключением исходных открытых ключей, можно хранить на стираемых носителях. В случае компрометации они восстанавливаются совместно всеми узлами в очередной фазе обновления. Так как исходный открытый ключ каждого узла необходим для восстановления данных узла после компрометации, он должен быть записан в ПЗУ.

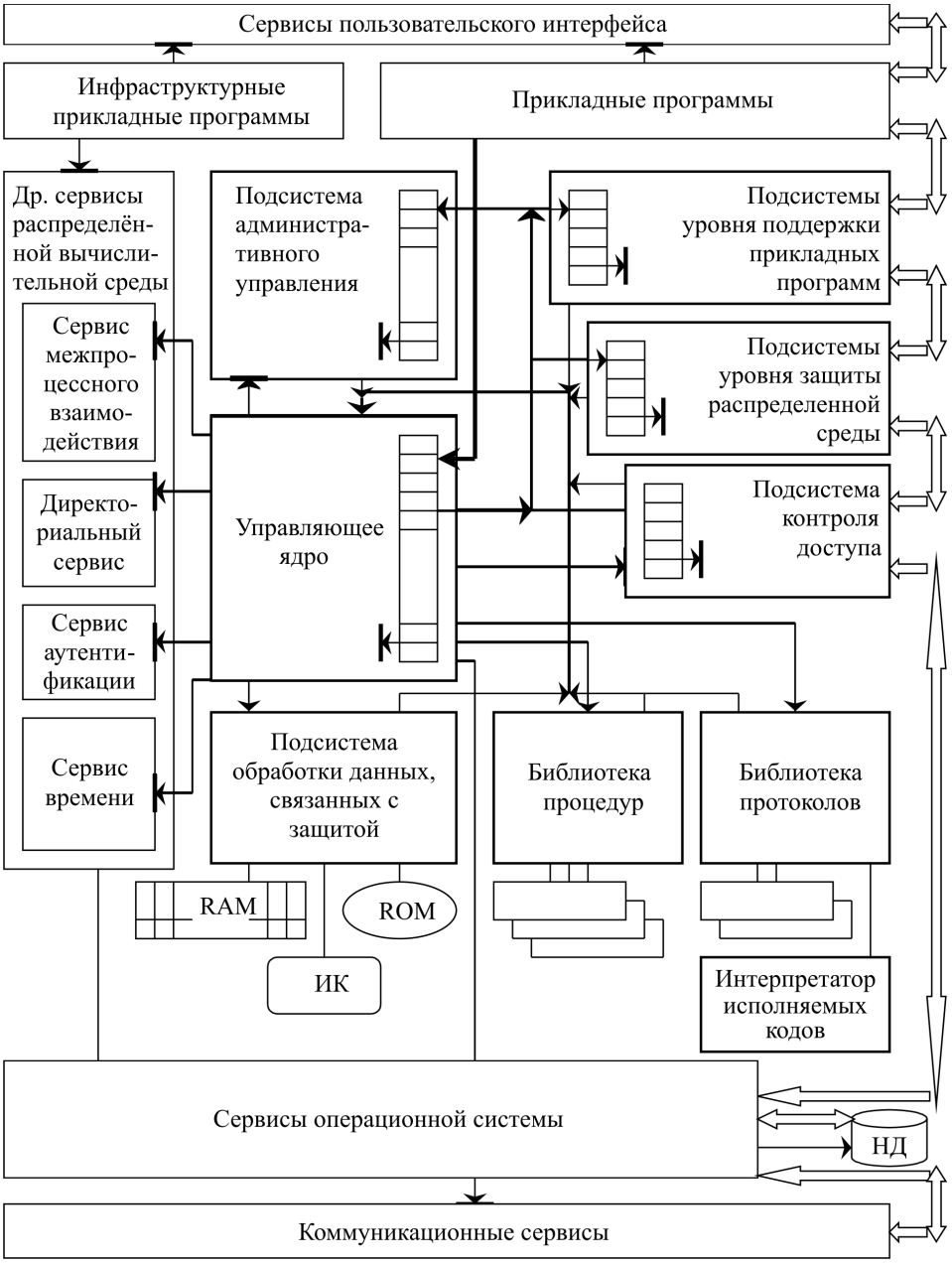

Рис. 1. Архитектура СКОИ. НД – носители данных; ИК – интеллектуальные карты; ROM – постоянное запоминающее устройство; RAM – системная область оперативной памяти

4. Заключение

Таким образом, предложенная структурно-функциональная модель позволяет реализовать многофункциональную многопользовательскую систему криптографической обработки информации, обладающую стойкостью к частичному разрушению ключевого материала и функционирующую в среде распределенных компьютерных систем. Разработанное алгоритмическое и протокольное обеспечение системы обеспечивает безопасность каждого используемого в ней криптографического ключа при одновременном разрушении не более t из общего числа n узлов системы, где $t \le [(n-1)/2]$. На основе предложенной модели разработаны основные элементы конструкции системы: ее архитектура, структурно-функциональное описание, принципы управления подсистемами, интерфейс прикладного программирования и интерфейсы подсистем, состав программного, информационного и аппаратного обеспечения.

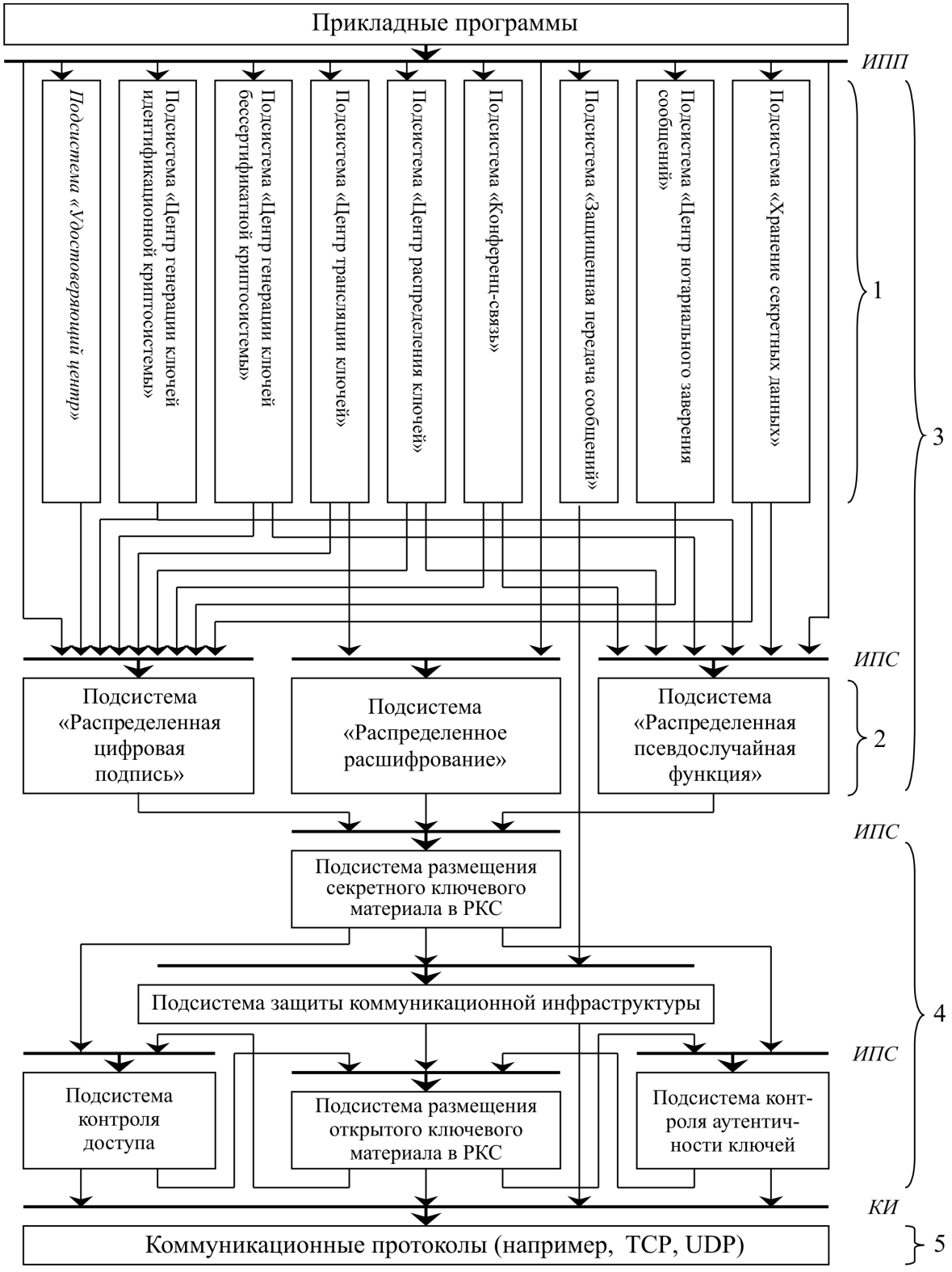

Рис. 2. Модульная структура алгоритмического обеспечения СКОИ:
1 – подсистемы, реализующие функции защиты ПП; 2 – подсистемы, выполняющие базовые функции защиты; 3 – «Уровень поддержки ПП» СКОИ; 4 – «Уровень защиты распределенной среды» СКОИ; ИПП – интерфейс прикладного программирования; ИПС – интерфейсы подсистем; КИ – коммуникационный интерфейс

Литература

1. Запечников С.В. Принципы обеспечения стойкости криптосистем к компрометации ключей // Безопасность информационных технологий. – 2008. – №1. – С. 80–87.

2. Запечников С.В. Защищенная рассылка сообщений в распределенных системах обработки данных в условиях действия активного адаптивного противника // Безопасность информационных технологий. – 2001. – №2. – С. 67–76.

3. Архангельская А.В. Схемы цифровой подписи на основе алгоритмов ГОСТ Р 34.10-2001 с применением аппарата парных отображений / А.В. Архангельская, С.В. Запечников // Известия Таганрогского государственного радиотехнического университета (ТРТУ). – 2006. – №7 (62). – С. 194–201.

4. Запечников С.В. Обеспечение криптографической стойкости при компрометации части ключей // Безопасность информационных технологий. – 2008. – №4. – С. 93–102.

5. Запечников С.В. Живучесть систем защиты информации как фактор обеспечения информационной и функциональной безопасности распределенных компьютерных систем // Безопасность информационных технологий. – 2005. – №4. – С. 8–17.

6. Запечников С.В. Модель «активной безопасности» и возможности ее реализации в системах криптографической защиты информации // Безопасность информационных технологий. – 1998. – №4. – С. 52–54.

Запечников Сергей Владимирович
Канд. техн. наук, доцент кафедры «Информационная безопасность банковских систем»
МИФИ, г. Москва
Тел.: (+7 495) 323-91-46 (раб.), (+7 916) 775-19-13 (моб.)
Эл. почта: oka@mephi.edu, SVZapechnikov@mephi.ru

S.V. Zapechnikov

The architectural and algorithmic framework for cryptographic information processing system keeping liveness in the adversarial environment

The purpose of the paper is to present an architectural and construction framework of a new universal cryptographic security system for distributed computing environment. A structural model and a high-level functional specification for the cryptographic security system are offered. The requirements for software, hardware and key management of the system are discussed.

Keywords: distributed computer systems, liveness, information security, cryptography, key management.
