ЗАЩИТА ИНФОРМАЦИИ

УДК 003.26

Т.В. Галибус, В.В. Краснопрошин

КОНЦЕПТУАЛЬНОЕ МОДЕЛИРОВАНИЕ И ОРГАНИЗАЦИЯ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Рассматриваются проблемы, связанные с организацией механизмов защиты информации в распределенных компьютерных системах. Предлагается двухуровневая иерархия моделей, которая позволяет упростить выбор эффективной стратегии защиты в зависимости от типа анализируемой системы. Строится модель сетевого механизма безопасности и формулируется методология последовательной настройки механизмов, согласованных с предложенной иерархией моделей.

Введение

В последнее время все большее число прикладных информационных систем (ИС) содержат в себе компоненты распределенной обработки информации [1, 2]. Таковыми, например, являются системы управления содержимым (content management), контроля версий, любые облачные платформы и сервисы и т. д. Современные ИС уже на этапе их проектирования ориентированы на глобальную информационную сеть, а значит, по умолчанию являются распределенными. Ключевые факторы уязвимости таких систем – всевозрастающие открытость и гибкость их инфраструктуры. Поэтому актуальной в настоящее время является проблема построения комплексной, надежной и всеобъемлющей системы защиты информации (СЗИ) [3].

Существует множество механизмов защиты, с помощью которых можно организовать систему безопасности, отвечающую различным целям [4]. Однако универсальной методики, которая позволяла бы снизить затраты на проектирование и автоматизировать процесс построения согласованной с конфигурацией распределенных компьютерных систем (РКС) системы защиты, к сожалению, нет [3, 5].

В работе предлагается подход, основанный на использовании формальных с точки зрения защиты информации моделей, который позволяет описывать различные конфигурации РКС и автоматизировать процесс построения соответствующих систем защиты. Использование формальных моделей дает возможность не только провести классификацию РКС и механизмов их защиты, но и оценить состояние защищенности самой системы.

Классификация общих информационных объектов с точки зрения защиты информации приведена в стандарте СТБ 34.101.30-2007 [6]. Авторами сформулирована специализированная методология проектирования СЗИ, в рамках которой предложена иерархия моделей и механизмов, в наибольшей степени подходящая для организации системы проектирования СЗИ и позволяющая автоматизировать процесс построения СЗИ для РКС в целом.

1. Общая модель распределенной информационной системы

Прежде чем сформулировать задачу на построение обобщенной СЗИ и определить методику ее решения, необходимо подробно рассмотреть объект защиты и определить характеристики, важные для построения такой системы.

Распределенные компьютерные системы появились в начале 1990-х гг. Они прошли определенный путь своего развития, при этом парадигма и технология их разработки неоднократно менялись [1].

По мнению многих авторов [2, 5, 7], базовыми составляющими, определяющими характер современных РКС на самом общем уровне, являются архитектура системы (А), сетевые технологии (Т) и тип управления системой (М).

Архитектура системы определяет структуру и состав системы, ее функциональное наполнение. Фактически она определяет общую взаимосвязь логической и физической структур системы и описывает организацию работы ее сервисных компонентов.

Коммуникационные технологии осуществляют связь между элементами системы и реализуют процесс обмена данными между приложениями на различных компьютерных системах и платформах.

Управление организует взаимодействие элементов системы (функционирование процессов внутри системы). Оно определяет степень централизации выполнения административных функций системы.

Принимая во внимание приведенные выше рассуждения и используя методологию построения концептуальных моделей, любую РКС формально можно записать в виде следующего кортежа:

$$C = (A, T, M).$$

При этом каждый компонент такой модели может принимать различные значения, определяя тем самым конфигурацию конкретной РКС. Ниже перечислены известные варианты указанных компонентов:

A_1. *Клиент-серверная архитектура.* Сервисы (сетевая нагрузка) в таких системах распределены между поставщиками услуг (серверами) и заказчиками услуг (клиентами). В силу высокой централизации компонентов такие системы, как правило, являются хорошо защищенными, но недостаточно гибкими. Кроме того, вероятность отказов в этих системах достаточно велика.

A_2. *Сервис-ориентированная архитектура* (СОА). В системах с такой архитектурой используются независимые или слабо связанные компоненты, ориентированные на выполнение конкретной функциональности (сервиса). Поставщиками и заказчиками услуг могут быть любые узлы сети, а четко определенный интерфейс сервиса и стандартизированный вызов обеспечивают независимость системы от программно-аппаратной платформы и вызывающего приложения. На сегодняшний день данный вид архитектуры практически является стандартом в корпоративных системах.

A_3. *Архитектура одноранговых сетей*. В данном случае все узлы сети являются равноправными участниками системы. При этом не существует четкой концепции выполнения конкретной функциональности. Такие системы характеризуются высокой гибкостью, но очень слабым уровнем защищенности.

A_4. *Архитектура грид*. Такая архитектура представляет собой объединение вычислительных ресурсов нескольких машин для решения трудоемких научных задач и проведения объемных вычислений. Компьютеры в этом случае объединяются в кластеры, и их ресурсы функционируют согласованно с целью выполнения операций, необходимых для решения поставленных задач. В таких системах отсутствует концепция сервиса (услуги). Данная архитектура не совсем подходит для коммерческих организаций и корпоративных сетей.

A_5. *Облачная архитектура*. Фактически является комбинацией СОА и грид-архитектуры. Иными словами, облачная архитектура представляет собой объединение ресурсов различных машин с целью выполнения конкретных функций. Данное объединение называется виртуализацией, поскольку поставщиком услуг фактически является виртуальный суперкомпьютер. В настоящий момент проблема стандарта безопасности для таких систем является наиболее актуальной как для международных, так и для государственных структур [8].

В настоящее время используются следующие типы коммуникационных технологий [1, 7]:

T_1. *Объектная технология* (CORBA, DCOM). Технологический стандарт и информационная технология для интеграции распределенных приложений на основе взаимодействия интерфейсов объектов. В большей степени соответствует архитектуре клиент – сервер.

T_2. *Компонентная* (CORBA, CCM). Дополняет объектную технологию стандартным каркасом приложения и набором стандартизированных интерфейсов (портов), при помощи которых приложения взаимодействуют в распределенной среде.

T_3. *Технология веб-сервисов* (SOAP, WSDL). Определяет межпрограммное взаимодействие на основе веб-стандартов при помощи веб-сервисов (программных систем, разработанных для поддержки интероперабельного взаимодействия через сеть). Соответствует архитектуре СОА

и является в настоящее время наиболее используемой технологией. Существует развернутый каталог стандартов безопасности веб-сервисов [9], который также включает стандарт интеграции грид-вычислений (OGSI) [10].

T_4. *Многоагентная технология* (KQML, ACL). Предполагает проектирование самоорганизующейся интеллектуальной системы на основе независимых самообучающихся программных агентов. Агенты общаются между собой при помощи специальных языков (протоколов). В силу слабой защищенности редко применяется для построения РКС.

T_5. *Технология* P2P. Модель взаимодействия равноправных узлов сети напрямую (без промежуточных серверов и экранов). В таких сетях отсутствуют какие-либо стандарты взаимодействия распределенных приложений; следовательно, данная технология может передавать данные согласно любому принятому протоколу. Соответствует архитектуре одноранговых сетей.

T_6. *Облачная технология.* Является развитием технологии веб-сервисов. Под этим термином понимается информационно-технологическая концепция (а не технология), гарантирующая наличие общего и повсеместного доступа по требованию к общему пулу вычислительных ресурсов. Согласно стандарту NIST основными свойствами такого пула являются эластичность, учет потребления, объединение ресурсов, самообслуживание по требованию, универсальный доступ по сети. Таким образом, в облачных технологиях используется целый комплекс технологий виртуализации, баланса нагрузки, интеграции ресурсов и приложений. В настоящее время не существует строгих стандартов облачных технологий (в отличие от веб-сервисов) [11], а сам этот термин начал применяться лишь в 2007–2008 гг.

Анализ указанных архитектур и технологий позволяет сделать вывод, что во многом эти компоненты ИС являются взаимосвязанными, поэтому переменная T в архитектурно-управленческой модели РКС важна лишь с точки зрения построения систем защиты, а не классификации РКС. Например, если для технологии веб-сервисов и соответствующих ей типов архитектур (клиент – сервер, СОА, грид) существует целая серия стандартов безопасности и сводов практик [9, 10, 12], то в области облачных систем и сервисов наблюдается значительный пробел, который требует своего решения [11, 8]. По этой причине в предложенной модели технологии для различного уровня взаимодействия сетевых сервисов, например CORBA и P2P, объединены в один компонент T.

Наконец, третий параметр – управление системами:

M_1. *Централизованное управление*. Подразумевает наличие в системе одного сервера с ограниченным доступом. Для большинства современных РКС такой вид управления является труднодостижимым идеалом.

M_2. *Частично централизованное управление*. Означает доступ ограниченного числа лиц и компьютерных систем. Часто встречается в корпоративных системах.

M_3. *Децентрализованное управление*. Характерно для наиболее открытых типов систем (P2P или общее облако). Безопасность информации в таких системах можно гарантировать лишь с помощью достаточно надежных криптографических методов защиты данных.

С учетом приведенных выше рассуждений любую РКС можно записать как функцию трех параметров:

$$DS = (A_i, T_j, M_k), \quad i = 1,...,5, \quad j = 1,...,6, \quad k = 1, 2, 3.$$

Подставляя в модель различные значения параметров, можно описывать различные конфигурации. Таким образом, концептуальные модели можно использовать для описания различных классов ИС с целью последующего их анализа.

Видно, что наиболее важной частью модели является ее архитектурно-технологическая составляющая. В соответствии с этой составляющей можно выделить пять базовых классов РКС: $K_1(A_3)$, $K_2(A_1)$, $K_3(A_2)$, $K_4(A_4)$, $K_5(A_5)$, а с учетом управляющей составляющей – восемь подклассов. Такая классификация распределенных систем позволит определить возможные механизмы, которые в дальнейшем можно использовать для построения системы их защиты. Опишем все указанные классы:

Класс K_1 – архитектура одноранговых сетей и технология P2P, в которых возможен лишь один уровень централизации управления:

M_3 – полностью децентрализованные системы. В силу отсутствия единого центра управления в таких системах практически невозможно обеспечить приемлемый уровень защищенности.

Класс K_2 – многочисленный класс клиент-серверных систем (им соответствует объектная, компонентная технология или технология веб-сервисов). В зависимости от уровня централизации управления можно выделить следующие его подклассы:

M_1 – полностью централизованные;

M_2 – частично централизованные (при наличии нескольких серверов).

В указанных подклассах необходимо обеспечить двухуровневую систему защиты – для серверов и клиентов. В силу высокого уровня централизации можно сравнительно легко обеспечить защиту таких систем. Основной проблемой остается высокая вероятность сбоев (низкая отказоустойчивость в силу отсутствия распределенной обработки данных) и отсутствие возможностей для масштабирования и расширения.

Класс K_3 – сервис-ориентированная архитектура, которой соответствует технология веб-сервисов. В зависимости от уровня централизации управления можно выделить следующий подкласс:

M_2 – частично централизованные системы.

В таких системах решение проблемы защиты информации эквивалентно обеспечению защиты сервисов (функций системы). Существуют технологические стандарты безопасности веб-сервисов и стандарты, определяющие механизмы защиты, а также общие принципы построения таких систем защиты. Основной проблемой в данном случае является разрозненность стандартов и повсеместное использование СОА, что требует в ситуациях, не описанных в стандартах, своевременного принятия технологичных и других решений.

Класс K_4 – архитектура и технология грид-вычислений. Возможны следующие варианты управления:

M_2 – частичное;

M_3 – децентрализованное.

Этот класс систем характеризуется разрозненностью стандартов и отсутствием эффективного технологичного решения проблемы безопасности [10, 12].

Класс K_5 – облачные системы и технологии. По уровню централизации управления их можно разбить на следующие подклассы:

M_1 – частично централизованные;

M_2 – полностью децентрализованные.

Основной проблемой в данном случае является отсутствие стандартов и критериев оценки защиты информации [11].

Таким образом, использование архитектурно-управленческих моделей позволяет провести классификацию РКС и выделить подклассы, в рамках которых достижимы различные уровни защиты информации. Классификация систем позволяет также согласовать механизмы защиты с критериями (методиками) решения и определить базис для построения комплексной системы защиты.

2. Выбор инфраструктуры безопасности

В основе большинства современных СЗИ лежат механизмы управления ключами, которые определяют базовую совокупность сервисов защиты информации [3, 4, 13], а все дополнительные механизмы и службы безопасности включаются в СЗИ уже в качестве ее надстройки. Ядром механизма управления ключами, как правило, является криптографический протокол проверки подлинности (ППП), который определяет концепцию доверия [13, 14]. Таким образом, можно считать, что механизм управления ключами (МУК) и ППП в совокупности определяют своеобразный базис СЗИ, т. е. своеобразную инфраструктуру ее безопасности.

Под инфраструктурой безопасности (ИБ) в дальнейшем будем понимать программно-аппаратную технологию, которая определяет механизмы аутентификации пользователей системы на основе ППП, МУК и механизмы согласования ключей между пользователями и сервисами системы.

Заметим, что понятие «инфраструктура безопасности» в различных литературных источниках именуется по-разному. Например, в монографии [14] оно определяется как «инфраструктура открытых ключей» (один из видов ИБ), а в монографии [3] серверы ключей и их функции неявно также удовлетворяют необходимым требованиям, а значит, являются прототипами ИБ. Можно также отметить, что отсутствует и какая-либо классификация технологий ИБ.

Вместе с тем анализ подходов к решению проблемы аутентификации и управления ключами позволяет сделать вывод, что в качестве базового множества ИБ можно принять следующие типы инфраструктур:

KI_1 – парольная инфраструктура;

KI_2 – инфраструктура протокола Kerberos;

KI_3 – инфраструктура открытых ключей;

KI_4 – инфраструктура открытых ключей (корпоративная);

KI_5 – собственная инфраструктура согласования ключей и функции аутентификации.

Каждая из перечисленных инфраструктур обладает как определенными достоинствами, так и недостатками и подходит только для конкретного типа архитектуры и уровня централизации РКС. Наиболее передовыми и надежными считаются технологии, связанные с инфраструктурой открытых ключей [14]. Однако их реализация в системах типа K_2 (клиент – сервер), как правило, является трудоемкой и неэффективной. В то же время инфраструктуры типа KI_3, KI_4 или KI_5 более пригодны для систем с удаленным доступом, т. е. для облачных технологий [11] (архитектур K_3, K_4, K_5) или для грид-технологий [12] и веб-сервисов [9]. В корпоративных сетях, основанных, как правило, на архитектуре K_2 или K_3, менее трудоемкой и независимой от времени доступа является реализация протокола и технологии управления ключами Kerberos (KI_2) или (при отсутствии у пользователя конфиденциальных данных (KI_1)) парольная инфраструктура:

	K_1	K_2	K_3	K_4	K_5
KI_1	+	+	–	–	–
KI_2	–	+	+	–	–
KI_3	–	–	+	+	+
KI_4	+	–	–	+	+
KI_5	+	+	+	+	+

Выбор инфраструктуры безопасности зависит также от степени централизации РКС. В централизованных, как правило, более защищенных системах достаточно присутствия единого сервера ключей Kerberos (KI_2) или, в исключительных случаях, парольной аутентификации KI_1. Для более распределенных систем следует использовать инфраструктуру KI_3 стороннего производителя (при малых ресурсах) или собственную внутреннюю инфраструктуру открытых ключей KI_4 (при большем количестве ресурсов). В случае большой степени распределенности данных и уровней доступа к системе возможно гибридное решение типа KI_5:

	KI_1	KI_2	KI_3	KI_4	KI_5
M_1	+	+			+
M_2	–	±	+	+	+
M_3	–	–	±	+	+

Выбор конкретной реализации зависит как от объемов располагаемых ресурсов, так и от степени конфиденциальности защищаемой информации. В нашей классификации трудоемкость реализации возрастает от KI_1 к KI_5. Защищенность сервера ключей, наоборот, уменьшается от KI_5 к KI_1.

Очевидно, что серверы ключей [3] независимо от реализации лишь частично решают проблему защиты информации в РКС. Например, они не решают важную задачу авторизации и организации списков доступа [3, 14]. Кроме того, в любой системе должен быть определен механизм аудита или протоколирования процессов, организации дополняющего (скрывающего) трафика, маршрутизации и т. д [4, 5]. Для решения этих задач, так же как и для уточнения базовой инфраструктуры, очевидно, необходимо провести уточнение архитектурно-управленческой модели на более низком компонентном уровне.

Таким образом, предложенная выше модель ИС позволяет определить только принципиальную инфраструктуру механизмов защиты и общий подход к оценке защищенности. Очевидно, что такую модель целесообразно использовать на этапе инициализации комплексной системы защиты. В большинстве случаев ее параметров недостаточно для определения конкретной конфигурации основных и дополнительных механизмов защиты, необходимых для отдельных элементов ИС (узлов, ресурсов, процессов сети и ее инфраструктуры).

3. Компонентная модель РКС

Формальный способ описания распределенных систем в виде концептуальных моделей позволил определить специализированную методологию построения системы их защиты. Для решения общей задачи защиты информации, как правило, применяется система стандартов ISO/IEC 15408 (В РБ СТБ 34.101.1-3) [15-17]. Однако для того чтобы согласовать конкретную РКС с набором ее средств защиты, необходимо перейти от общего описания классов к их детальному наполнению. На важность компонентного подхода в решении задачи безопасности для открытых систем указывает и специализированный стандарт сетевой безопасности под названием «Интерпретация общих критериев защищенных систем для сетевых конфигураций» [18]. Основными компонентами (объектами) распределенной системы, как правило, являются:

– ресурсы (R);
– узлы (N);
– процессы (Pr).

Таким образом, концептулаьную модель системы на компонентном уровне можно представить в виде следующего кортежа:

$$C = (R, N, Pr).$$

К ресурсам относятся программный код или аппаратные средства, используемые в РКС:

– данные, хранящиеся в системе;
– сервисы, т. е. функциональные возможности, которые система предоставляет пользователям;
– узлы сети за исключением клиентов, т. е. потребителей информации;
– коммуникационные каналы сети.

К узлам системы относятся все подключенные к ней устройства. При этом в зависимости от типа архитектур возможны несколько типов таких устройств:

– клиенты, т. е. потребители информации и сервисов;
– серверы, т. е. устройства, обеспечивающие функциональность сети;
– устройства хранения данных;
– пиры – узлы, которые могут иметь функциональность на уровне клиента или сервера.

Процессами в системе являются любые исполняемые на узлах сети и передаваемые по ее коммуникационным каналам программные коды:

– информационные потоки сервисов;
– пользовательские процессы (сервисы);
– внутренние процессы управления системой;
– защитные процессы.

В качестве основной единицы процесса моделирования будем рассматривать узлы сети.

Пусть в сети имеется k узлов:

$$N = (N_1, ..., N_k).$$

Предположим, что в узлах сети хранятся некоторые наборы данных, т. е. каждому узлу N_i соответствует набор данных $(D_1,\ldots,D_{t(i)})$:

$$N_i \rightarrow D_i = (D_1,\ldots,D_{t(i)}).$$

Переменные D_j означают метки безопасности данных узла. Метки безопасности определяют уровни секретности, поддерживаемые системой, и образуют упорядоченные множества, например: «совершенно секретно», «секретно», «несекретно» и «для общего доступа». Отметим, что в общем случае метки безопасности должны быть приведены в соответствие с СТБ 34.101.30 [6]. В различных системах категории доступа и наборы меток безопасности могут отличаться друг от друга. Таким образом, набору данных в системе в общем случае соответствует матрица $k(t)$, где t – общее число меток безопасности.

Очевидно, матрица каналов для k узлов связи содержит k^2 значений. Каждому каналу, соединяющему узлы N_i и N_j , присваивается метка его безопасности:

$$Ch = (Ch_{11},\ldots,Ch_{k,k}).$$

При наличии между узлами нескольких каналов их также можно задать наборами меток.

Для определения процессов и сервисов системы введем функцию *Pr* (*Send, Receive*), где компонента *Send* определяет вектор, задающий подмножество узлов (N_{i1}, …, N_{is}), которые передают матрицу данных (D_{i1}, …, D_{is}), а компонента *Receive* – соответственно вектор и матрицу данных узлов-получателей. Таким образом, в общем случае процесс представляется в виде двух подматриц набора данных системы.

С учетом приведенных рассуждений каждую систему на данном компонентном уровне можно задать в виде тройки

$$SDS = (D, Ch, Pr),$$

где D определяет матрицу меток безопасности данных узлов сети, Ch – матрицу меток безопасности каналов сети, а Pr – совокупность пар подматриц матрицы D.

Видно, что описанная выше модель позволяет определить необходимый уровень безопасности каждого компонента системы, поскольку требуемый уровень (профиль) безопасности определяется новым защищенным состоянием системы:

$$SDS_{pr} = (D_{pr}, Ch_{pr}, Pr_{pr}),$$

где D_{pr} – набор защищенных данных системы, т. е. измененная матрица меток безопасности с учетом функциональности добавленных механизмов. Пусть при анализе системы выяснилось, что в некотором узле в открытом доступе хранятся данные, которые нужно сделать конфиденциальными. После реализации механизма шифрования защищенность этих данных повысится, а значит, соответствующее значение в матрице меток поменяется;

Ch_{pr} – набор защищенных каналов. После добавления функциональности механизмов безопасности в системе могут появиться новые, более защищенные каналы связи, которые могут быть организованы при наличии базовой инфраструктуры при помощи безопасного обмена ключами симметричного или асимметричного шифрования;

Pr_{pr} – набор процессов защищенной системы, который также включает в себя процессы, относящиеся к механизмам безопасности.

Результатом решения задачи защиты информации (ЗЗИ) является переход РКС из текущего состояния *SDS* в состояние SDS_{pr}. Видно, что модель РКС на компонентном уровне позволяет оценить текущее состояние системы *SDS* и выбрать необходимые механизмы безопасности с целью реализации целостной СЗИ, обеспечивающей состояние системы SDS_{pr}.

Отметим, что принятие решения о выборе механизмов безопасности является, по сути, оптимизационной задачей, поскольку на выбор механизмов влияет не только вероятность осуществления угроз, но и стоимость затрат на реализацию механизмов. Таким образом, предложенный подход к решению задачи обеспечения защищенного состояния РКС тесно связан с традиционной методикой оценки рисков безопасности.

Таким образом, иерархия моделей *DS* и *SDS* (на архитектурно-управленческом и компонентном уровнях) дает возможность определять объекты защиты, их основные характеристики и требуемый уровень защиты, что позволит ставить и решать ЗЗИ в распределенной системе. В первую очередь для решения данной задачи необходимо определить инструменты или средства защиты РКС, которые базируются на выбранной инфраструктуре безопасности в соответствии с классом РКС.

4. Механизмы и функции обеспечения безопасности

Для того чтобы построить систему защиты, необходимо определить не только объект защиты, но и средства защиты [4]. Объектом защиты является модель распределенной системы *SDS* или кортеж компонентов системы в совокупности с характеристикой класса системы *DS*. Механизмы безопасности (*Meh*) по признаку принадлежности к сервисам безопасности (семейству взаимосвязанных механизмов для предоставления определенной защитной функции) делятся на следующие группы:

– аутентификация;
– управление доступом;
– конфиденциальность данных;
– целостность данных;
– предотвращение отказа от авторства.

Помимо сервисов имеются непосредственные механизмы безопасности, которые могут относиться к сервисам или поставляться отдельно:

– шифрование;
– цифровая подпись;
– механизмы разграничения доступа;
– механизмы контроля целостности;
– протоколы взаимной аутентификации;
– подстановка трафика;
– управление маршрутизацией;
– механизм заверения;
– доверенная функциональность;
– метки безопасности;
– обнаружение событий;
– аудит безопасности;
– восстановление безопасного состояния.

Для того чтобы выбрать набор механизмов или средств безопасности для конкретной распределенной системы из доступного множества, необходимо сформировать базовое множество алгоритмических (*Alg*) и технических (*Prot*) средств [3, 4, 11]. Каждый из этих механизмов, по сути, представляет собой совокупность процессов, в которых принимают участие компоненты (узлы, данные, процессы) системы, т. е. которым обеспечивается определенное свойство системы на компонентном уровне. Например, аутентификация – это поддержка процессов проверки подлинности пользователей системы. Таким образом, в наиболее общем виде механизм *M* можно описать как вектор (кортеж)

$$Meh = (T, Pr_1, Pr_2, \ldots, Pr_n, Scene),$$

где T – применяемая технология (*Alg* или *Prot*); $\{Pr_1, Pr_2, \ldots, Pr_n\}$ – совокупность процессов механизма; *Scene* – совокупность участников функционирования механизма, ресурсов (D_{scene}), каналов (Ch_{scene}) и процессов (Pr_{scene}), т. е. часть системы на компонентном уровне, имеющая отношение к реализации или протокола:

$$Scene = (D_{scene}, Ch_{scene}, Pr_{scene}).$$

Результатом действия механизма является изменение состояния сцены, т. е. $Meh\ (T, Pr_1, \ldots, Pr_n, Scene) = Scene_{pr}$, где $Scene_{pr}$ – защищенное состояние подмножества компонентов системы. Видно, что в результате действия последовательности механизмов $Meh_1, \ldots, Meh_k$ вся система

перейдет в состояние SDS_{pr}. Следует отметить, что ключевыми в сетевых конфигурациях являются криптографические механизмы ($T = Alg$), поскольку именно они гарантируют доступ к данным независимо от операционной системы и устройства.

Выбор механизмов безопасности зачастую представляет собой задачу принятия решения. Для решения подобных задач, как правило, используются экспертные оценки и методы.

5. Методика построения СЗИ

В основе описанного выше концептуального подхода лежит выбор средств защиты в зависимости от класса и компонентного состава РКС. Такая методология обобщает известные ранее подходы к защите информации открытых систем, основанные прежде всего на выборе конкретных механизмов, ориентированных на решение некоторых подзадач ЗЗИ, т. е. покрывающих лишь часть необходимой функциональности комплексной СЗИ [13, 14]. Это затрудняло поиск наиболее эффективного решения для данного класса систем. В соответствии с обобщенной формулировкой ЗЗИ (см. разд. 2) предлагается следующая поэтапная методика проектирования СЗИ:

1. Идентификация класса системы, т. е. определение параметра DS.
2. Выбор класса инфраструктуры безопасности и базовой комплектации сервисов безопасности.
3. Идентификация компонентов системы, т. е. определение параметра *SDS*.
4. Уточнение требований к уровню защиты (SDS_{pr}).
5. Инициализация механизмов защиты M_i в зависимости от выбранных технологий и в соответствии с достижимым уровнем защиты.
6. Настройка параметров механизмов на конкретную систему (решение оптимизационной задачи).

Необходимым условием проектирования является аппаратная и системная независимость такой СЗИ. Следовательно, наиболее предпочтительными средствами и методами защиты служат криптографические механизмы [13], надежность которых не зависит от каналов связи, узлов сети и доступа конечных пользователей.

Прикладные аспекты построения комплексной системы защиты ранее не являлись актуальной ЗЗИ, поскольку не все компоненты РКС находились в открытом доступе, а систем, в полной мере удовлетворяющих характеристикам распределенности, практически не существовало. В нынешних условиях необходимость в создании аппаратно-, платформо- и каналонезависимых средств защиты возрастает в силу значительного роста популярности и использования облачных систем и сервисов, которые, по сути, являются открытыми и децентрализованными системами [8, 11].

Применение методики идентификации системы с последующей оптимизационной настройкой параметров позволит эффективно и точно решать проблему безопасности открытых систем в короткие сроки.

Рассмотрим решение проблемы защиты информации на примере ИС с распределенной облачной инфраструктурой. Пусть известен исходный класс системы (облачный), тип управления (частично централизованный, корпоративный) и основные цели системы (хранение данных, управление доступом). В соответствии с описанным выше подходом можно достаточно точно определить настройки системы безопасности.

Первый уровень иерархии – *архитектурный*. Он включает следующие этапы:

1. Выбор типа аутентификации. Для рассматриваемой системы хранения данных необходима двухфакторная аутентификация. Так как в системе имеются данные, доступ к которым нужно ограничивать, аутентификацию предлагается проводить с помощью пароля и доступа к почтовому ящику (мобильному устройству).

2. Выбор инфраструктуры безопасности. Для систем с облачной инфраструктурой необходимо использовать уровень защиты не ниже шифрования с открытым ключом. Поскольку требуется шифровать большие объемы данных, принято решение использовать гибридную систему шифрования: для защиты пользовательских сессионных ключей – инфраструктуру PKI, а для шифрования самих файлов – AES128.

Второй уровень иерархии – *компонентный*. Настройка дополнительных механизмов в разных системах осуществляется по-разному:

1. В облачных сервисах авторизация должна быть независимой от платформы и типа устройства. Кроме того, на выбор типа авторизации влияют дополнительные факторы, такие как скорость шифрования, тип организации пользовательских групп доступа, стоимость реализации и т. д. С учетом этого был выбран оптимальный для таких сервисов тип авторизации: шифрование с атрибутами, модифицированное с учетом особенностей системы.

2. На сервере организуется аудит всех событий, происходящих в системе.

Описанная концепция безопасности реализована в рамках выполнения реального прикладного проекта. Базовая конфигурация механизмов была выбрана в соответствии с двухуровневой методологией; система безопасности состояла из четырех компонентов – клиента, сервера и хранилища файлов и ключей. Сервер в данном случае призван поддерживать функциональность ИС, а клиент – защищать данные на устройствах пользователей, при этом клиент с хранилищем файлов и ключей напрямую не взаимодействует.

Заключение

В работе описан один из возможных подходов к построению СЗИ в РКС. Рассмотрены основные архитектуры распределенных систем, соответствующие механизмы безопасности и принципы построения СЗИ. Построена иерархия формальных (концептуальных) моделей, которая позволяет описывать различные классы и конфигурации ИС. На первом (архитектурно-управленческом) уровне иерархии определяется база СЗИ, т. е. инфраструктура безопасности, которая включает способы аутентификации и установления безопасного соединения. Более тонкие механизмы, к которым относятся авторизация, настройка маршрутов и аудит данных, определяются на втором (компонентном) уровне.

В отличие от существующих подходов, которые опираются на выбор совокупности независимых механизмов, предлагаемая методология построения СЗИ носит специализированный характер. Также описана целостная концепция безопасности систем с облачной инфраструктурой, указана пошаговая стратегия выбора и конфигурирование механизмов безопасности.

Таким образом, в работе предложена методология, которая позволяет упростить и автоматизировать процесс проектирования СЗИ в соответствии с целями и особенностями РКС. Результаты работы обсуждались и получили признание на Международной научной конференции консорциума IEEE [19].

Список литературы

1. Таненбаум, Э. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. – СПб. : Питер, 2003. – 877 с.

2. Косяков, М.С. Введение в распределенные вычисления / М.С. Косяков. – СПб. : НИУ ИТМО, 2014. – 155 с.

3. Фергюсон, Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М. : Диалектика, 2004. – 432 с.

4. О некоторых вопросах технической и криптографической защиты информации : Приказ Оперативно-аналитического центра при Президенте Республики Беларусь, 30 авг. 2013 г. № 62 // Нац. реестр правовых актов Респ. Беларусь. – 2015. – № 3. – 22 с.

5. Галатенко, В.А. Стандарты в области безопасности распределенных систем / В.А. Галатенко // Jet Info. – 1999. – № 5. – С. 98–99.

6. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация : СТБ 34.101.30–2007. – Введ. 01.04.08. – Минск : Межгос. совет по стандартизации, метрологии и сертификации : Белорус. гос. ин-т стандартизации и сертификации, 2007. – 7 с.

7. Радченко, Г.И. Распределенные вычислительные системы / Г.И. Радченко. – Челябинск : Фотохудожник, 2012. – 184 с.

8. Galibus, T. Cloud Storage Security / T. Galibus, H. Vissia // Proc. of NSCE’2014, 24–25 December 2014. – Hong Cong : CRC Press, 2015. – P. 123–127.

9. OASIS Web Services security Technical Committee and standardization group [Electronic resource]. – 2015. – Mode of access : https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss. – Date of access : 19.10.2015.

10. Open Grid Services Infrastructure (OGSI) Specification Version 1.0 [Electronic resource]. – 2003. – Mode of access : http://xml.coverpages.org/OGSI-SpecificationV110.pdf. – Date of access : 21.10.2015.

11. Cloud Security Alliance, organization promoting the use of best practices for providing security assurance within Cloud Computing [Electronic resource]. – 2015. – Mode of access : https://cloudsecurityalliance.org. – Date of access : 11.10.2015.

12. A Security Architecture for Computational Grids / I. Foster [et al.] // Proc. 5th ACM Conf. on Computer and Communications Security. – N.Y., 1998. – P. 83–92.

13. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

14. Полянская, О.Ю. Инфраструктуры открытых ключей / О.Ю. Полянская, В.С. Горбатов. – М. : Бином, 2007. – 216 с.

15. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель : СТБ 34.101.1–2014 (ISO/IEC 15408–1:2009). – Введ. 01.09.14. – Минск : Межгос. совет по стандартизации, метрологии и сертификации : Белорус. гос. ин-т стандартизации и сертификации, 2014. – 53 с.

16. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности : СТБ 34.101.2–2014 (ISO/IEC 15408–2:2009). – Введ. 01.09.14. – Минск : Межгос. совет по стандартизации, метрологии и сертификации : Белорус. гос. ин-т стандартизации и сертификации, 2014. – 178 с.

17. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности : СТБ 34.101.3–2014 (ISO/IEC 15408-3:2009). – Введ. 01.09.14. – Минск : Межгос. совет по стандартизации, метрологии и сертификации : Белорус. гос. ин-т стандартизации и сертификации, 2014. – 131 с.

18. Trusted Network Interpretation NIST security standard [Electronic resource]. – 2015. – Mode of access : http://csrc.nist.gov/publications/secpubs/rainbow/tg005.txt. – Date of access : 17.10.2015.

19. Krasnoproshin, V. Conceptual Distributed System Models and Organization of Security Mechanisms / V. Krasnoproshin, T. Galibus // Proc. of 8th Intern. IEEE Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Application (AIDAACS'2015), 24–26 September. – Warsaw, Poland, 2015. – P. 432–43.

Поступила 13.11.2015

Белорусский государственный университет,
Минск, пр. Независимости, 4
e-mail: tan2tan@gmail.com
krasnoproshin@bsu.by

T. Galibus, V. Krasnoproshin

CONCEPTUAL MODELLING AND ORGANIZATION OF SECURITY MECHANISMS IN DISTRIBUTED SYSTEMS

We analyze the existing DS from the point of security and construct a two-level hierarchy of models. Such approach allows us to separate the abstraction (architecture) level and the concrete (component) level of ISS. The core set of methods, i. e. authentication and key exchange protocols, corresponds to the abstraction level and is defined as security infrastructure (SI). The final security parameters optimization and additional mechanisms such as authorization, routing and data auditing of the protection mechanisms are configured on the component level of the DS. In addition, we outline the systematic step-by-step ISS configuration method.