Доверенная среда облачных вычислений

К. Б. Здирук,
А. В. Зотова,
С. А. Петренко,
М. П. Сычев

В настоящее время Cloud Computing (облачные вычисления) являются одной из ключевых тем отечественной государственной программы «Информационное общество (2011–2020)». Министерство связи и массовых коммуникаций РФ проводит конкурсы на проектирование единой сети передачи данных для федеральных органов власти РФ и создание пилотных решений «государственного облака». Ожидается, что облачные технологии позволят существенно повысить эффективность использования вычислительных ресурсов организации, сократить операционные расходы, улучшить управляемость и устойчивость корпоративной информационной системы в целом. При этом вопросы защиты информации облачных технологий по-прежнему остаются открытыми. Давайте посмотрим, какие возможные пути организации доверенной среды облачных вычислений существуют на практике.

Введение в проблему

Как правило, под «облаком» понимается некоторая совокупность вычислителей, объединенных в единый вычислительный ресурс с использованием технологий виртуализации [1, 3]. При этом на одном вычислителе могут находиться несколько пользовательских виртуальных машин. Возможный прогноз развития облачных технологий представлен на рис. 1.

К основным характеристикам (рис. 2) облачных вычислений относятся следующие.

1. Общая инфраструктура – использование технологий виртуализации позволяет отделить физическую среду. Это обеспечивает меньшую связность вычислительных ресурсов с компонентами серверов, тем самым делая решение более гибким.

2. Динамическое выделение ресурсов (масштабируемость) – с помощью приложения по управлению ресурсами автоматически выделяются дополнительные ресурсы либо уменьшается доступный ресурс по требованию.

3. Сетевая доступность – возможность подключиться к выделенным ресурсам извне.

4. Управляемый учет – возможность вести учет и управление потребляемых ресурсов для оптимизации их использования.

Выделяют три основные модели облачных служб (рис. 3):

- «программное обеспечение как услуга» (Software as a Service – SaaS);
- «платформа как услуга» (Platform as a Service – PaaS);
- «инфраструктура как услуга» (Infrastructure as a Service – IaaS).

В модели SaaS пользователю доступны только функциональные возможности некоторого приложения из «облака».

В модели PaaS пользователю разрешается установить и использовать

некоторое приложение на платформу. При этом существует ряд ограничений на возможность настройки операционной системы, сетевых устройств и пр.

В модели IaaS пользователь получает контроль над операционной системой, приложениями, сетевыми ресурсами и интерфейсами, но не над инфраструктурой «облака» в целом.

Также выделяют следующие модели развертывания облачных служб:

- частное «облако» (Private cloud);
- «облако» сообщества (Community cloud);
- общее (или публичное) «облако» (Public cloud);
- гибридное «облако» (Hybrid cloud).

Частное «облако» – инфраструктура, предназначенная для использования одной организацией, включающей в себя несколько потребителей (например, подразделений одной организации), а также, возможно, клиентами и подрядчиками данной организации. Частное «облако» может находиться в собственности, управлении и эксплуатации как самой организации, так и третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

Публичное «облако» – инфраструктура, предназначенная для свободного использования широкой публикой. Оно может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное «облако» физически существует в юрисдикции владельца – поставщика услуг.

Гибридное «облако» – это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений (например, кратковременное использование ресурсов публичных «облаков» для балансировки нагрузки между «облаками»).

Общественное «облако» – вид инфраструктуры, предназначенный для использования конкретным со-

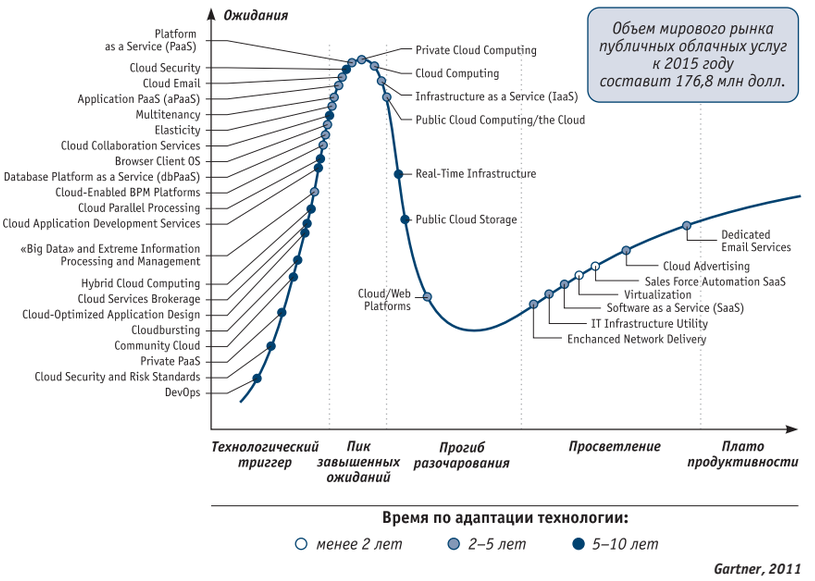

Рис. 1. ***Цикл развития облачных технологий***

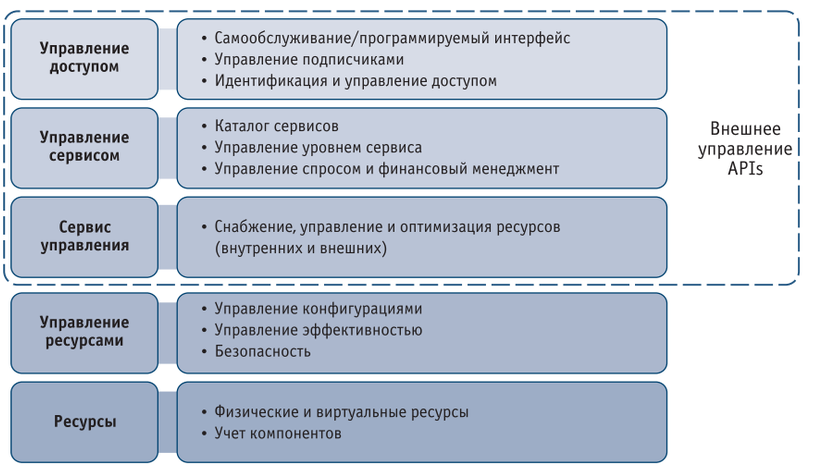

Рис. 2. ***Пример характеристик «облака»***

Рис. 3. ***Основные понятия и определения облачных технологий***

обществом потребителей из организаций, имеющих общие задачи (например, миссии, требований безопасности, политики и соответствия различным требованиям). Общественное «облако» может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или более организаций, входящих в сообщество, или третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца.

Основными компонентами облачных технологий являются гипервизор и средства управления и мониторинга. Гипервизор – это аппаратная или компьютерная схема, обеспечивающая виртуализацию. Он позволяет на одном компьютере параллельное выполнение многих независимых операционных систем и управление ими, эмулируя при этом аппаратное обеспечение. Тем самым гипервизор позволяет перейти от физического подхода к логическому.

Гипервизоры делятся на следующие типы:

- автономный гипервизор (гипервизор типа 1) работает непосредственно на оборудовании системы;
- на основе базовой ОС (гипервизор типа 2) – такие гипервизоры работают поверх основной операционной системы, которая обеспечивает поддержку устройств ввода/вывода, управление памятью, а также процессорным временем.

В первом случае гипервизор работает с физическим оборудованием: он управляет памятью, выделяет вычислительные ресурсы и т. д. Зачастую они представляют собой доработанную операционную систему, которая предоставляет возможность более глубокого управления ресурсами физического оборудования. В качестве примера можно рассмотреть платформу VMWare ESX/ESXi.

Во втором случае гипервизору, который является программным обеспечением, устанавливаемым на полноценную операционную систему, приходится работать с ресурсами, выделенными ему операционной системой. Пример – система KVM. Средства управления представляют собой программные продукты, которые позволяют вести точную настройку большого количества гипервизоров, управление резервированием, миграцией и состоянием виртуальных машин.

Проблема безопасности возникает из-за того, что появляется некоторый новый слой (а в случае гипервизора типа 2 – два новых слоя), которые могут нести угрозы. Становится необходимым обеспечить защиту как основной ОС (в случае использования гипервизора типа 2), так и гипервизора. Несмотря на то что система виртуализации должна изолировать гостевые среды, гарантировать это в общем случае нельзя. Происходит так потому, что, например, взаимодействие между несколькими виртуальными машинами, находящимися на одном физическом оборудовании, происходит через виртуальные сетевые интерфейсы внутри гипервизора, то есть – через общую память. Как следствие, возможны следующие типовые атаки на облачные вычислители:

- атака на гостевую систему;
- атака на гипервизор, которая позволяет получить доступ к памяти других гостевых систем, выполняющихся на данном сервере, а также управлять им (атака происходит из другой гостевой системы, которая находится на данном сервере);
- атака на гипервизор, которая позволяет получить доступ к памяти других гостевых систем, выполняющихся на данном сервере, а также управлять им (атака происходит извне);
- атака на основную операционную систему, позволяющая добиться полного контроля над сервером (в случае гипервизора типа 2).

Возможный подход к решению проблемы

При выборе программно-аппаратных платформ облачного вычислителя для критически важного объекта (далее – КВИУС), как правило, возникает противоречие между, с одной стороны, вынужденной необходимостью применения заимствованных технологий и готовых решений для получения на выходе паритетных функциональных характеристик проектируемых отечественных образцов, а с другой – реальной угрозой отказа системы и (или) невыполнения требований информационной безопасности на этапе ее эксплуатации.

Таким образом, одной из ключевых проблем создания доверенной облачной среды вычислений является решение вопроса о принципиальной допустимости и способах применения, в общем случае, недоверенных программно-аппаратных средств и компонентов в его составе.

Объекты КВИУС могут оснащаться разнородными аппаратно-программными платформами (АПП), функционирующими в составе защищенных центров обработки данных (ЦОД), выделенных специализированных серверов, а также рабочих станций (в том числе – мобильных). Неизбежным следствием при этом являются две возникающие задачи: интеграции разнородных информационно-вычислительных ресурсов и реализации унифицированной модели защиты процессов и данных в составе гетерогенных КВИУС.

Возможный подход формирования доверенной облачной вычислительной среды базируется на основе включения в АПП *доверенного* общесистемного программного обеспечения (ОСПО), в состав которого, наряду с компонентами интеграции разнородных приложений, обмена данными и управления вычислительным процессом, входят унифицированные программные средства защиты информации.

Доверенное программное обеспечение (ДПО) предполагает выполнение следующих условий:

1) авторизации кода (подтвержденной независимым органом) и 100-процентного правообладания им резидентами РФ (юридическими и/или физическими лицами);

2) представления полного состава конструкторской и программной документации в соответствии с ГОСТ Российской Федерации;

3) сопровождения процессов проектирования, разработки и сертификации программного кода внеш-

ним уполномоченным органом (Министерством обороны РФ, ФСТЭК России, ФСБ России).

Условно-доверенное программное обеспечение (УПО) предполагает невыполнение хотя бы одного из условий определения ДПО. *Недоверенным программным обеспечением* (НПО) считается код, в отношении которого не выполняются все три вышеперечисленных требования (так называемые «обобщенные критерии доверия» (ОКД).

Для аппаратного обеспечения (*hardware*) аналогичным образом могут быть определены соответствующие классы ДАО, УАО и НАО.

Примечание 1. *В ряде случаев показатель качества (комплексная мера существенных свойств, определяющих пригодность для целевого применения [1]) недоверенных компонентов превосходит аналогичные показатели для элементов условно-доверенного и доверенного классов.*

Отнесение любого элемента или АПП в целом к классу *недоверенных* или *условно-доверенных* средств с точки зрения предлагаемого подхода не исключает его применения в составе КВИУС. Данное противоречие может быть преодолено посредством формирования *доверенной вычислительной среды* (ДВС), функционирующей в составе произвольной АПП с поддержкой интероперабельности процессов хранения, обработки и обмена данными.

В этом случае функции хранения, обработки и передачи конфиденциальной информации должны исполняться процессами, погруженными в доверенную среду, изоляция которой от внешних и внутренних вредоносных воздействий должна быть обеспечена на уровне *встроенного периметра защиты* (ВПЗ) [6].

Модель организации доверенной облачной среды

Формирование доверенной облачной вычислительной среды (ДВС), защищенной от угроз нарушения доступности, целостности и конфиденциальности основывается на выборе системы аксиом начального уровня, базовых сущностей и принятых ограничений.

Без потери общности решения включим *условно-доверенные* средства в класс *недоверенных*, в рамках дальнейшего изложения ограничимся рассмотрением самых распространенных и, как представляется на сегодняшний день, наиболее уязвимых АПП, оснащенных процессорами x-86 архитектуры с поддержкой аппаратной виртуализации (АПП-АВ). В качестве средств базовой ОС будем рассматривать недоверенную среду на базе открытого ядра UNIX.

Необходимо построить целевую систему таким образом, чтобы исключить возможность реализации множества угроз $\{УГ_i\}$, возникающих при совместном функционировании доверенных и недоверенных компонентов в составе АПП-АВ.

АПП нами рассматривается как совокупность конечных непересекающихся множеств доверенных $\{KD\}$ и недоверенных $\{KS\}$ программных компонентов, распределенных по иерархическим уровням вложенных слоев P_i, $i = 0(1)N$, в основании которых лежит слой P_0 – доступ к физическим (не виртуализируемым) аппаратным ресурсам. Вычислительный процесс, понимаемый как преобразование входного информационного потока в выходной, в общем случае распределен между различными слоями в соответствии с доступным для каждого слоя P_i множеством функциональных возможностей (сервисов) $\{C_j\}$, $j = M_j - 1 + 1\ (1)\ M_j$, разрабатываемых с применением объектно-ориентированных методов (инкапсуляции, наследования и полиморфизма).

Вводится следующая система аксиом.

Аксиома 1. В АПП может быть выделен слой P_0, реализуемый *только доверенными* средствами. Вычислительная среда, построенная в P_0, является безопасной и защищенной (адекватной всем предполагаемым угрозам).

Аксиома 2. Слои P_i, $i = 1(1)N$ являются по определению уязвимыми и недоверенными, при этом предполагается возможность как внутреннего, так и внешнего несанкционированного доступа, в результате которого могут быть нарушены доступность, целостность и конфиденциальность информации, хранящейся и обрабатываемой на вычислительной установке.

Аксиома 3. Доверенные компоненты в составе произвольного слоя P_i, $i = 1(1)N$ функционируют внутри периметра защиты данного слоя и взаимодействуют с соседними слоями посредством защищенных программных (API) интерфейсов.

Зададим дополнительные требования (группы А и Б), выполнение которых при условии принятия аксиом 1–3 обеспечит достаточный уровень защиты от угроз информационной безопасности (ИБ) в произвольной АПП.

А. Общие требования.

Обеспечение доступности.

А-1. Слой P_0 должен поддерживать рекуррентные методы контроля, управления и восстановления исполнения доверенных процессов слоев P_i, $i = 1(1)N$.

Обеспечение целостности.

А-2.1. Слой P_0 должен поддерживать рекуррентные методы контроля целостности доверенных компонентов слоев P_i, $i = 1(1)N$ и циркулирующей информации между ними.

А-2.2. Для каждого слоя P_i, $i = 1(1)N$ его целостность и изоляция доверенных компонентов обеспечивается доверенными средствами слоя P_{i-1}.

Обеспечение конфиденциальности.

А-3.1. Должна быть обеспечена единая идентификация доверенных и недоверенных программных компонентов, функционирующих в составе АПП.

А-3.2. Для всех слоев P_i, $i = 0(1)N$ должна поддерживаться унифицированная дискреционная и мандатная модель управления доступом программных компонентов к защищаемым ресурсам (информационным, программным и аппаратным) [3].

Специальные требования группы Б сформулированы на основе угроз ИБ для АПП-АВ (рис. 4). Слева на рисунке показана классическая архитектура АПП и адекватная ей модель наложенной системы защиты. Справа – угрозы ИБ, обусловленные включением в состав АПП

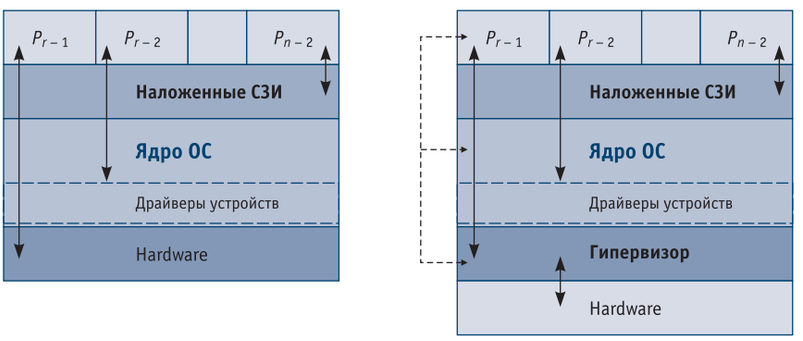

Рис. 4. ***Актуальные угрозы ИБ для АПП с поддержкой технологий аппаратной виртуализации***

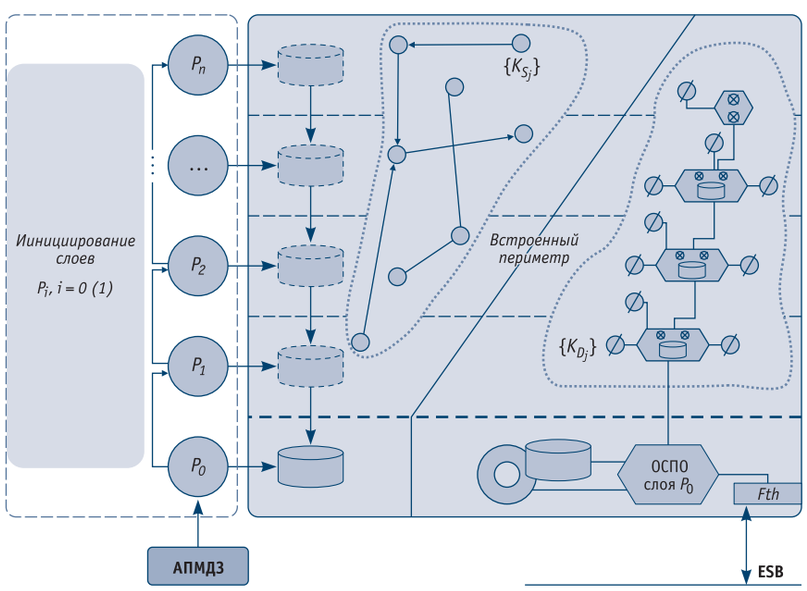

Рис. 5. ***Схема организации совместного функционирования доверенных и недоверенных компонентов в составе АПП***

привилегированных инструкций (команд) аппаратной виртуализации для переключения в режим *гипервизора* (*root-operation*) с доступом к управляющим регистрам виртуализации.

Б. Специальные требования (для АПП-АВ).

Б-1. Конфиденциальные данные должны размещаться *только* в слое P_0. Непосредственный (то есть с нарушением требования А-2.2) доступ к защищенным информационным ресурсам слоя P_0 для всех слоев P_i, $i = 1(1)N$ должен быть исключен.

Б-2. Слои P_i, $i = 1(1)N$ должны гарантированно изолироваться от слоя P_0 средствами архитектуры АПП (набора инструкций и прерываний процессора). Выдача привилегированных инструкций аппаратной виртуализации недоверенными программными компонентами должна блокироваться.

Б-3. Инициирование программных компонентов слоя P_0 должно выполняться внешними сертифицированными средствами доверенной загрузки. Инициализация слоев P_i, $i = 1(1)N$ производится в последовательности: $P_0 \rightarrow P_1 \rightarrow \ldots \rightarrow P_N$.

Схема организации совместного функционирования доверенных и недоверенных компонентов для слоев P_i, $i = 0(1)N$ в составе АПП приведена на рис. 5.

Организация функционирования на каждом слое P_i, $i = 0(1)N$ множества его доверенных компонентов $\{KD\}_i$ реализуется средствами общесистемного программного обеспечения «промежуточного» слоя (обозначается аббревиатурой ОСПО или термином *middleware*), включающими в свой состав унифицированные кросс-платформенные компоненты организации распределенной обработки, хранения, обмена данными и управления безопасностью [7]. Унифицированная (*каноническая*) схема вычислительного процесса для доверенных компонентов (рис. 6) инвариантна отношению к АПП и различным слоям P_i в их составе.

Схема поддерживается на каждом узле неоднородной вычислительной сети, при этом все интерфейсы взаимодействия между распределенными *KD*-компонентами унифицируются на уровне ОСПО (*middleware*) таким образом, что симметричное взаимодействие распределенных (на множестве различных слоев P_i одной или различных АПП) приложений сводится к композиции локальных обращений к ОСПО-*агентам* и взаимодействию *агентов* между собой по внутреннему защищенному протоколу (ESB-шине).

Для дальнейшего рассмотрения вопросов организации защищенного взаимодействия между доверенными компонентами $\{KD\}$ одного и/или различных слоев P_i, $i = 1(1)N$ введем обозначения:

- $<a_j, a_k>$ – бинарное отношение, представляющее однонаправленный интерфейс взаимодействия двух различных доверенных элементов с индексами $(j, k) \neq 0$ внутри произвольного i-слоя множества $\{KD\}_i$, $i = 1(1)N$;
- a_0 – доверенный компонент ОСПО данного слоя.

Тогда отображение:

$RL : \{<a_j, a_k>\} \rightarrow \{<a_j, a_0> \lozenge \lozenge <a_0, a_k>\}$

является биекцией ($\forall\ j \neq k$).

Утверждение 1 (У-1).

Вычислительная среда, построенная в соответствии с системой аксиом 1–3, общими и специальными требованиями (А, Б) и канонической схемой организации функционирования доверенных компонентов для каждого слоя P_i, $i = 0(1)N$, является безопасной и защищенной (адекватной всем предполагаемым угрозам), при этом количество интерфейсов, необходимых для реализации полносвязного взаимодействия k-доверенных элементов одного слоя, минимально (для $k \geqslant 3$).

Примечание 2. *Для множества {KS} (см. рис. 5), содержащего k-элементов, нижняя граница количества интерфейсов определяется как* C_k^2, *для множества {KD} она линейно зависит от его мощности – |KD|.*

В АПП, поддерживающих технологию аппаратной виртуализации, может иметь место как вертикальное, так и горизонтальное масштабирование слоев виртуальной архитектуры (виртуальных машин) в рамках одного или различных узлов ЛВС в составе КСА объекта, связанных посредством *интероперабельных* средств ОСПО P_0-слоя(ев) и ESB-шины.

Определение (О-1).

Интероперабельность – свойство сохранения стабильности структурной организации (S), реализуемых функций (F) и интерфейсов (I) программного компонента $K = <S, F, I>$ при его функционировании в составе гетерогенных АПП.

С учетом данного определения бинарным отношением вида $<a_j, b_k>$ может представляться однонаправленный интерфейс взаимодействия различных доверенных элементов (с индексами j, k), принадлежащих масштабированным множествам $\{KD\}a$ и $\{KD\}b$ в рамках одного или различных узлов ЛВС объекта (a_0 и b_0 – интероперабельные доверенные компоненты ОСПО множеств $\{KD\}a$ и $\{KD\}b$ соответственно).

Биективность отображения $(\forall\ (a_j, a_0) \in \{KD\}a, \forall\ (b_k, b_0) \in \{KD\}b)$ $RG: \{<a_j, b_k>\} \rightarrow \{<a_j, a_0> \lozenge <a_0, b_0> \lozenge \lozenge <b_0, b_k>\}$ – множества однонаправленных интерфейсов на множество композиций бинарных отношений с учетом тождественности отношения $<a_0, b_0>$ позволяет сформулировать

Утверждение 2 (У-2).

Масштабированная вычислительная среда в условиях действия У-1 является безопасной и защищенной (адекватной всем предполагаемым угрозам), при этом количество интерфейсов, необходимых для реализации полносвязного взаимодействия доверенных элементов различных масштабированных множеств $\{KD\}a$ и $\{KD\}b$ посредством интероперабельных компонентов ОСПО, минимально (для $l = \min\{|KD|a, |KD|b\} \geqslant 2$).

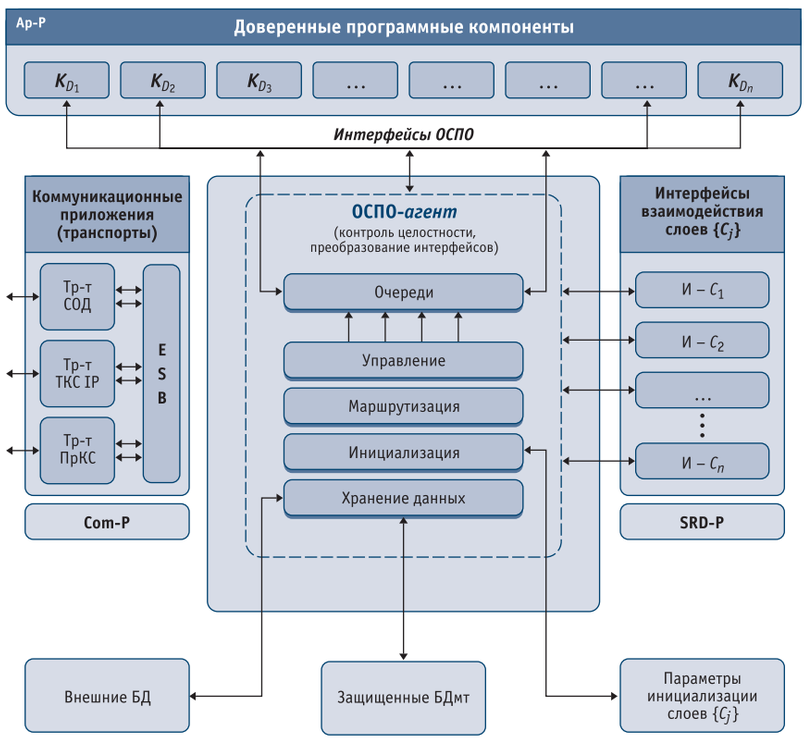

Рис. 6. ***Каноническая схема организации защищенной обработки данных***

Реализация гарантированной защиты вычислительных и информационных ресурсов ЦОД от вредоносного воздействия (как внешнего, так и внутреннего), изоляция процессов обработки данных в виртуальных средах различных уровней конфиденциальности, контроль и управление функционированием всей виртуальной инфраструктуры являются необходимыми условиями перехода к доверенной архитектуре облачных вычислений. По мнению авторов, выполнение предложенного комплекса общих и специальных требований на основе системы аксиом 1–3 для АПП, поддерживающих режим аппаратной виртуализации, позволяет реализовать в составе КВИУС функционально полный и непротиворечивый механизм гарантированного перехвата диспетчером доступа всех обращений субъектов к объектам доступа, при этом гарантии основываются на архитектуре АПП (в соответствии с требованиями РД ФСТЭК России для СВТ 1 класса защищенности). ■

ЛИТЕРАТУРА

1. NIST. Определение облачных вычислений [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

2. Уинклер Вик. Облачные вычисления: Вопросы безопасности в виртуальных облаках [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/ruru/magazine/hh641415.aspx.

3. Безопасная сегментация в унифицированной архитектуре центров обработки данных Cisco [Электронный ресурс]. – Режим доступа: http://www.cisco.com/web/RU/downloads/broch/white_paper_.pdf.

4. Ronald L. Krutz, Russel Dean Vines, Cloud Security: Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, 2011.

5. Здирук К. Б., Астрахов А. В., Лонский А. В. Модель защиты информации в гетерогенных вычислительных сетях на базе архитектуры встроенных «защищенных контуров» // Труды X Российской научно-технической конференции «Новые информационные технологии в системах связи и управления», 1–2 июня 2011 г. – Калуга, 2011, с. 543–545.

6. Здирук К. Б. Вопросы организации защищенной системы хранения и обработки данных в гетерогенных вычислительных сетях // Вопросы защиты информациик. 2007, № 3 (78), с. 6–9.

7. Андреев В. В., Здирук К. Б. ИВК Юпитер: реализация корпоративной политики безопасности в вычислительных сетях // Открытые системы. 2003, №№ 7–8, с. 43–46.