D. A. Postoev

Information-flow-based Access Control for Virtualized Systems

Keywords: virtualization, data protection tools development, access control, information flow control, security model

The article is devoted to the method of information-flow-based access control, adopted for virtualized systems. General structure of access control system for virtual infrastructure is proposed.

Д. А. Постоев

УПРАВЛЕНИЕ ДОСТУПОМ В ВИРТУАЛЬНЫХ СИСТЕМАХ НА ОСНОВЕ КОНТРОЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ

Введение

Согласно стратегии развития отрасли информационных технологий до 2020 г., виртуализация наряду с облачными вычислениями является одним из наиболее перспективных направлений [1]. Повышенный интерес к технологиям виртуализации в настоящее время неслучаен, их применение позволяет увеличить эффективность использования вычислительных ресурсов, сократить расходы на инфраструктуру, а также упростить управление, масштабирование и обеспечить отказоустойчивость системы.

Однако внедрение технологий виртуализации требует пересмотра вопросов безопасности. Попытки построить защиту, используя те же подходы, что и для «физических» систем, не приведут к нужному результату, так как виртуализация добавляет новые компоненты, которые также нуждаются в дополнительном контроле.

Согласно требованиям регуляторов, подсистема управления доступом в виртуальной системе должна включать в себя управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин [2, 3]. Контроль доступа в операционной системе осуществляется с помощью уже имеющихся решений, сформированных для «физических» систем. Для того чтобы построить подсистему управления доступом для виртуальной среды, рассмотрим ее архитектуру и функции.

Архитектура виртуальной инфраструктуры

В большинстве виртуальных систем можно выделить следующие составные части (рис. 1):

1) серверы виртуализации;
2) виртуальные машины;
3) сервер управления виртуальной инфраструктурой;
4) система хранения данных;
5) АРМ администраторов;
6) рабочие места пользователей виртуальной инфраструктуры;
7) сеть передачи данных.

Центральным элементом виртуальной инфраструктуры являются серверы виртуализации с установленным на них гипервизором. Гипервизор — это программа, создающая среду функционирования других программ (в том числе других гипервизоров) за счет имитации аппаратных средств вычислительной техники, управления этими средствами и гостевыми операционными системами, функционирующими в данной среде [4].

Сами виртуальные машины представляют собой набор файлов, хранящих конфигурацию оборудования и данные в виде файлов жестких дисков и снапшотов (мгновенных снимков виртуальной машины). Виртуальные машины обычно хранятся в общих для серверов виртуализации хранилищах данных, что позволяет им свободно перемещаться для распределения нагрузки и обеспечения отказоустойчивости.

Сервер управления виртуальной инфраструктурой позволяет управлять всеми элементами системы: серверами виртуализации, виртуальными машинами, сетевыми хранилищами и сетью.

В зависимости от обрабатываемых данных и их назначения выделяют несколько видов сетей. Для организации доступа администраторов к объектам виртуальной инфраструктуры используется сеть администрирования, по ней осуществляется передача управляющих команд от клиента с рабочего места администратора к серверу управления виртуальной инфраструктурой или серверу виртуализации.

Перейдем к рассмотрению общего подхода к управлению доступом в виртуальной среде.

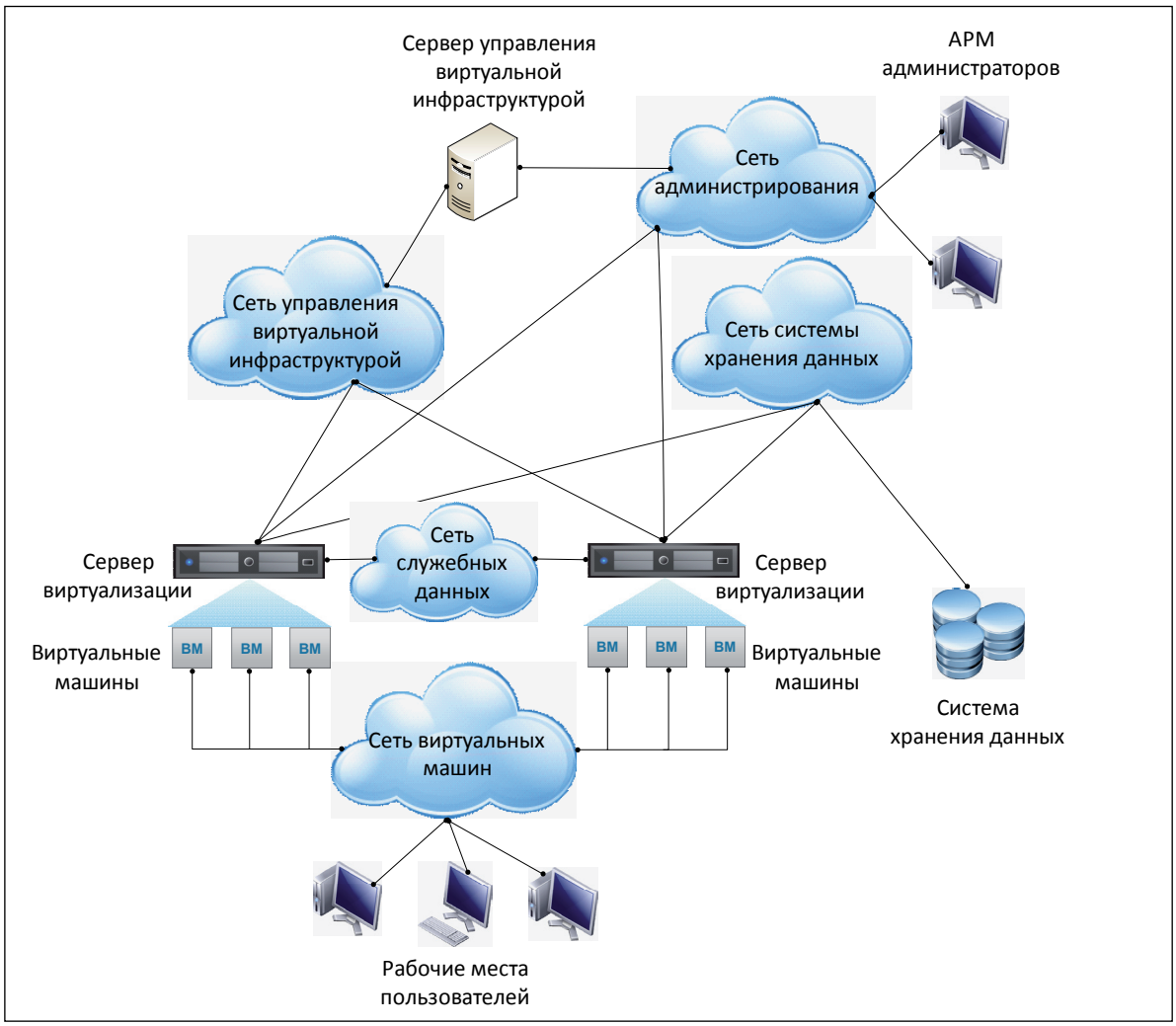

Рис. 1. Архитектура виртуальной инфраструктуры

Теория управления доступом в виртуальной среде

Функция безопасности, которая контролирует, как пользователи и компоненты информационной системы взаимодействуют с другими компонентами и ресурсами, называется управлением доступом. Теорию управления доступом будем строить на основе контроля информационных потоков.

Информационный поток представляет собой запрос на выполнение операций, направленных на изменение состояния целевого объекта. В виртуальных системах существует два вида информационных потоков, создаваемых при исполнении команд управления: от субъектов доступа к объектам (поток типа «субъект-объект») и между объектами виртуальной инфраструктуры (поток типа «объект-объект»).

Определение 1. Потоком типа «субъект-объект» называется информационный поток, связанный с выполнением инициатором команды управления над целевым объектом.

Определение 2. Потоком типа «объект-объект» называется информационный поток, связанный с изменением состояния объектов, участвующих в исполнении команды управления.

В виртуальной среде инициатором является пользователь (администратор), имеющий доступ к интерфейсу управления виртуальной инфраструктурой. В качестве целевых объектов выступают элементы системы виртуализации, описанные ранее (виртуальные машины, хранилища, хосты).

Решение о предоставлении доступа принимается на основе предиката предоставления доступа. Введем следующие обозначения:

пусть U — множество пользователей, R — множество операций, O — множество объектов доступа, $u \in U$ – инициатор запроса, $r \in R$ – запрашиваемое действие; $T \subset O$ – множество целевых объектов для данной команды.

1. Иерархические метки:

$(I; \leq)$ — шкала уровней доступа к информации, на основе иерархических меток;

level: $U \to I$ — функция уровней доступа пользователей;

level: $O \to I$ — функция уровней конфиденциальности объекта.

2. Неиерархические метки:

L — множество неиерархических меток, L_u — множество неиерархических меток, принадлежащих пользователю u; L_t — множество неиерархических меток, принадлежащих объекту t, где $t \in T$.

3. Предикат «операция доступа разрешена».

M — матрица доступов, $A \subset R$, $A = M[u, t]$; A — множество разрешенных пользователю u операций над объектом t.

То есть если $r \in A$, то операция считается разрешенной. Таким образом, предикат «операция доступа разрешена» записывается:

$$f_D(r,u,T) = \bigwedge_{t \in T} D(r,u,t), \text{ где:}$$

$$D(r,u,t) = \begin{cases} 1, & r \in M[u,t]; \\ 0, & r \notin M[u,t]. \end{cases}$$

4. Предикат «поток типа “субъект-объект” разрешен».

Поток типа «субъект-объект» называется разрешенным, если:

1. Уровень иерархической метки инициатора не ниже уровня метки объекта;

2. Множество неиерархических меток объекта является подмножеством неиерархических меток пользователя.

$$f_{SO}(u,T) = \bigwedge_{t \in T} f_{SO}(u,t) = \bigwedge_{t \in TF} \{ I_{SO}(u,t) \wedge L_{SO}(u,t) \}, \text{где:}$$

$$I_{SO}(u,t) = \begin{cases} 1, & level(u) \geq level(t); \\ 0, & level(u) < level(t). \end{cases} \qquad L_{SO}(u,t) = \begin{cases} 1, & L_t \subset L_u; \\ 0, & L_t \not\subset L_u. \end{cases}$$

5. Предикат «поток типа “объект-объект” разрешен».

Поток типа «объект-объект» называется разрешенным, если выполняется требование информационного невлияния [5], то есть все объекты, участвующие в нем, имеют одинаковые уровни доступа. Поэтому предикат «поток типа “объект-объект” разрешен» будет записан:

$$f_{OO}(u,T) = \bigwedge_{t_i,t_j \in T} I_{OO}(t_i,t_j), \text{ где:}$$

$$\text{Для } \forall i,j : t_i,t_j \in T,\ t_i \neq t_j \ \rightarrow I_{OO}(t_i,t_j) = \begin{cases} 1, & level(u) = level(t); \\ 0, & level(u) \neq level(t). \end{cases}$$

Команды управления могут относиться к нескольким объектам или использовать их в качестве параметров. Для каждого объекта данной операции по отдельности решается, будет предоставлен доступ или нет. Если хотя бы для одного объекта команды доступ запрещен, запрещается исполнение всей команды. Для каждой тройки инициатор-объект-операция доступ разрешается при истинности трех предикатов: предиката «операция доступа разрешена», предиката «поток типа “субъект-объект” разрешен» и предиката «поток типа “объект-объект” разрешен».

Предикат предоставления доступа записывается:

$f\ (r,\ u,\ T) = f_D(r,\ u,\ T) \wedge f_{OO}(u,\ T) \wedge f_{SO}(u,\ T)$, то есть доступ предоставляется, если потоки типа «субъект-объект» и «объект-объект» являются разрешенными и операция доступа разрешена в матрице доступов.

Общая схема системы управления доступом на основе контроля информационных потоков

Администрирование виртуальной инфраструктуры происходит с рабочих мест администраторов с помощью специального клиента, который подключается к серверу управления виртуальной инфраструктурой или отдельным серверам виртуализации через сеть администрирования. Таким образом, для перехвата и управления информационными потоками необходимо расположить между рабочими местами администраторов и сервером управления (серверами виртуализации) сервер контроля информационных потоков.

Так как сетевое соединение между клиентом и сервером устанавливается по защищенному протоколу HTTPS, необходимо реализовать поддержку SSL/TLS на прокси-сервере. Для клиента управления прокси-сервер представляется сервером управления виртуальной инфраструктурой и устанавливает, после запроса сертификатов и обмена ключами, защищенное SSL-соединение. Затем прокси-сервер соединяется с сервером управления и, представляясь ему клиентом, устанавливает второе соединение. Таким образом, мы получаем возможность перехватывать и расшифровывать трафик, посылаемый с клиента на сервер управления.

Полученное после расшифровки HTTP-сообщение поступает в модуль принятия решения о предоставлении доступа, в котором происходят его анализ и обработка и выделение из него информации, необходимой для принятия решения. На основе этой информации принимается решение о предоставлении или отказе в доступе инициатору в установлении доступа к целевому объекту. После либо запрос передается целевому объекту, либо инициатору посылается сообщение об отказе в доступе (рис. 2).

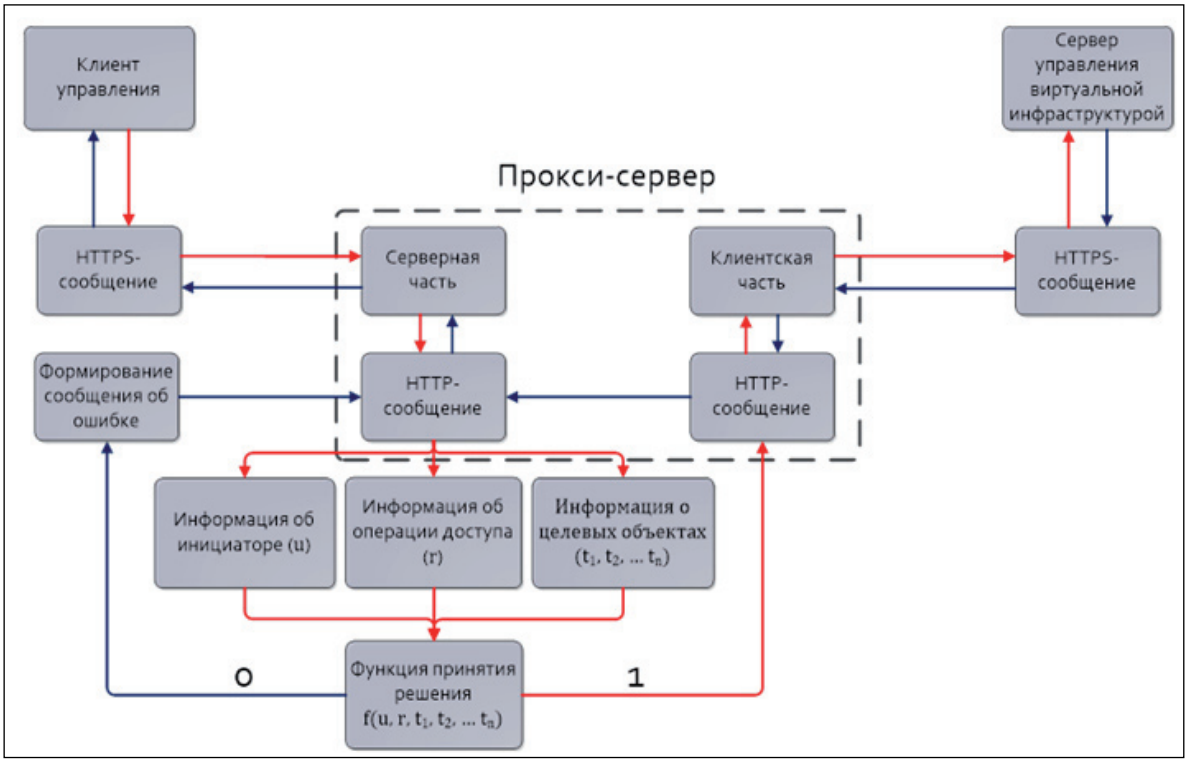

Рис. 2. Структура модуля управления доступом

Заключение

Для решения задачи контроля доступа в виртуальной инфраструктуре рассмотрены основные функции системы управления доступом и структура ее модулей. Были проанализированы особенности разграничения доступа в виртуальных системах, основные объекты, а также операции, используемые в подобных информационных системах. Были выделены типы информационных потоков, определены критерии разрешенных потоков и выработаны правила разграничения доступа на их основе. Полученные в результате исследования методы защиты выражены в виде общей схемы системы управления доступом. Данный подход позволяет реализовать модуль защиты, выполняющий требования регуляторов по управлению доступом в виртуальных системах.

СПИСОК ЛИТЕРАТУРЫ:

1. Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года (утв. распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р).
2. Приказ № 17 ФСТЭК России от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
3. Приказ № 21 ФСТЭК России от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
4. Проект ГОСТ Р XXXXX-20XX. Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации.
5. *Девянин П. Н.* Модели безопасности информационных потоков // Модели безопасности компьютерных систем: Учебное пособие для студентов высших учебных заведений. М.: Изд. центр «Академия», 2005. С. 55–66.

REFERENCES:

1. Strategiya razvitiya otrasli informatsionykh tekhnologiy v Rossiyskoy Federatsii na 2014–2020 gody i na ρerspectivu do 2025 goda (utv. rasρoryazheniyem Ρravitelstva Rossiyskoy Federatsii ot 1 noyabrya 2013. № 2036-ρ).
2. Ρrikaz № 17 FSTEK ot 11 fevralya 2013 g. "Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsyonnykh sistemakh".
3. Ρrikaz № 21 FSTEK ot 18 fevralya 2013 g. "Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer ρo obespecheniyu bezoρasnosti ρersonalhykh dannykh ρri ikh obrabotke v informatsionnykh sistemakh ρersonalnykh dannykh".
4. Ρroekt GOST Ρ XXXXX-20XX. Zashchita informatsii, obrabatyvaemoy s ispolzovaniem tekhologii virtualizatsii.
5. *Devyanin Ρ. N.* Modeli bezoρasnosti informatsionnykh ρotokov // Modeli bezoρasnosti informatsionnykh system: Uchebnoye ρosobie dlya studentov vysshykh uchebnykh zavedeniy. M.: "Akademiya", 2005. Ρ. 55–66.