В.С. Кузнецов

Модель защиты облачного сервиса на основе модели открытой среды OSE/RM

В статье предложен алгоритмический подход к построению модели защиты облачного сервиса. В качестве основы представления облачной системы автором выбрана модель открытой среды OSE/RM, которая позволяет систематизировать и обосновать выбор механизмов защиты.

Для демонстрации возможности практического применения предложенного алгоритма построения модели защиты строится его модифицированное расширение, позволяющее адаптивно выполнять верификацию модели защиты облачной среды.

Ключевые слова: модель защиты, облачный сервис, модель открытой среды, верификация модели защиты.

В настоящее время разрабатываются разнообразные подходы к обеспечению безопасности информационных систем. Существует масса средств их реализации как программными и аппаратными механизмами, так и организационными мерами. Особую актуальность обретает системный подход к обеспечению информационной безопасности. В работе предлагается в качестве основного средства систематизации использовать эталонную модель POSIX OSE/RM, которая позволяет обосновать выбор адекватных механизмов защиты и сформулировать алгоритм построения модели защиты облачного сервиса.

Согласно определению IEEE POSIX 1003.0, открытой информационной системой (далее – ОИС) называется система, которая реализует открытые спецификации на интерфейсы, сервисы (услуги среды) и поддерживаемые форматы данных, достаточные для того, чтобы дать возможность должным образом разработанному прикладному программному обеспечению быть переносимым в широком диапазоне систем с минимальными изменениями, взаимодействовать с другими приложениями на локальных и удаленных системах и взаимодействовать с пользователями в стиле, который облегчает переход пользователей от системы к системе.

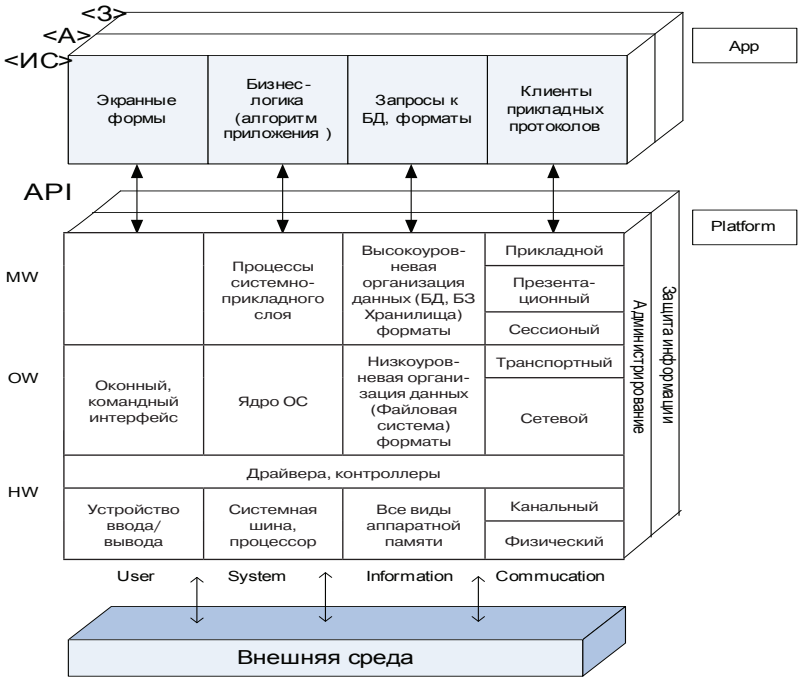

Рис. 1. Концептуальная модель OSE/RM

Подходы, описанные в стандарте[1], продолжают активно применяться, что дает основания использовать указанную модель при решении задач, связанных с обеспечением информационной безопасности (далее – ИБ).

Модель ОИС (рис. 1) представляется сочетанием платформенной и прикладной компонент, а также проекций базовой плоскости <ИС> на плоскость защиты <З> и администрирования <А>. Функциональное обслуживание представлено следующими видами услуг[2]: услуги, реализуемые операционной системой, услуги интерфейса «человек–машина», услуги организации данных, услуги, реализуемые столбцом System, сетевые услуги.

Кроме перечисленных видов услуг, существуют дополнительные, встроенные во все основные услуги: защиты информации, административного управления, а также набор инструментальных средств.

Данная модель реализует сервисный подход к представлению информационной системы (ИС), который на сегодняшний день

является наиболее прогрессивным. Его идея заключается в том, что ИС в целом представляется иерархией сервисов: прикладная компонента App – средство реализации бизнес-сервисов, которыми пользуются конечные пользователи, платформенная компонента – совокупность системных сервисов, необходимых для функционирования приложений. Если сервис – это используемый кем-то объект, то он должен опубликовать свой интерфейс (способ обращения к нему) для своих независимых пользователей. Системные сервисы предоставляются посредством API-функций, структурированных в соответствии с референсной функциональностью колонок модели OSE/RM.

Взгляд на ИС с позиции представления ее как средства реализации бизнес-процессов органично вписывается в современную парадигму развития вычислительных средств, парадигму, в которой на смену классическим ИС с ограниченным периметром и заданной заранее топологией приходят системы облачных вычислений. Облачные вычисления, согласно определению NIST[3], это модель обеспечения повсеместного и удобного сетевого доступа по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам – как вместе, так и по отдельности), которые могут быть оперативно предоставлены и освобождены с минимальными эксплуатационными затратами и/или обращениями к провайдеру. На сегодняшний день облачные вычисления представляют собой новую парадигму информационных технологий. В западных странах деятельность всех участников информационного взаимодействия в рамках технологии облачных вычислений регламентирована в достаточной степени, что обеспечивает прозрачность и повышает эффективность данной технологии.

Потребитель услуг облачного провайдера, ориентируясь на потребности своих бизнес-процессов, арендует необходимые вычислительные мощности либо программное обеспечение. Таким образом, потребитель видит ИС, решающую его прикладные задачи, исключительно как совокупность бизнес-процессов, абстрагируясь от аппаратных ограничений. Поскольку бизнес-процессы потребителя выполняются на стороне провайдера облачных вычислений, остро встает вопрос защиты данных. С точки зрения защиты, представление ИС как совокупности бизнес-процессов говорит о том, что свойства, обеспечивающие безопасность бизнес-процессов, должны быть распространены на «клетки» всех плоскостей модели OSE/RM (рис. 2)[4]: т. е. для реализаций «клеток» базовой плоскости модели должны обеспечиваться свойства безопасности,

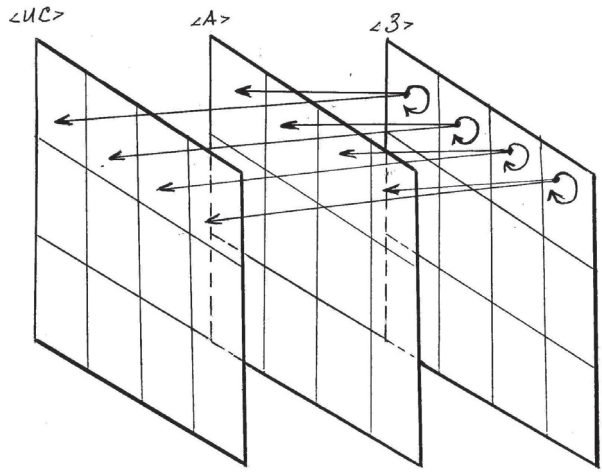

Рис. 2. Обеспечение безопасности клеток модели OSE/RM

аналогично для реализаций «клеток» плоскости администрирования <А> и защиты <З>.

В работе[5] автором продемонстрирована принципиальная возможность использования модели OSE/RM для описания облачной системы. Главной особенностью, отличающей модель OSE/RM классической ИС от модели облачного сервиса, является взаимодействие ИС потребителя облачных услуг и ИС провайдера. Бизнес-процессы потребителя облачных услуг выполняются как на стороне принадлежащих ему ИС, так и на стороне провайдера облачных услуг. В результате модель OSE/RM должна аккумулировать в себе (рис. 3) модели ИС провайдера и потребителя.

Таким образом, задача защиты информации в облачной системе эквивалентна задаче защиты набора бизнес-процессов, реализующих облачный сервис, на протяжении всех «клеток» его расположения в модели OSE/RM (рис. 3), поскольку информационные атаки в рамках ОИС представляются аналогичным образом в виде набора цепочек[6].

Оригинальный стандарт[7] описывает функции плоскости защиты достаточно поверхностно. ИБ в стандарте только обозначена как совокупность межкатегорийных защитных сервисов, что не дает возможности использовать референсное представление функциональности данной плоскости модели при построении модели защиты. Подходы, предложенные в стандарте, были расширены

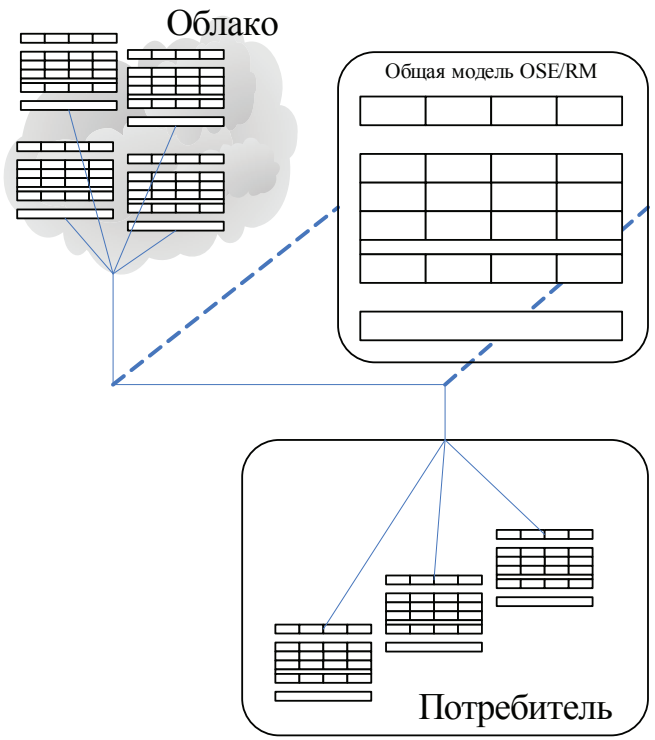

Рис. 3. Модель облачного сервиса

рядом авторов[8], что дает возможность использовать референсное представление плоскости защиты для решения прикладных задач ИБ.

Для обеспечения ИБ ОИС представим облачный сервис как совокупность бизнес-процессов. Любой бизнес-процесс, выполняемый в ОИС, реализует 4 вида операций над данными: хранение данных, обработка данных, передача данных (через носители информации), передача данных (через сеть). Всякая операция над данными однозначно определяется набором «клеток» модели OSE/RM, участвующих в ее функционировании.

Всякий механизм защиты реализуется в определенном наборе «клеток» модели ОИС. «Клетки» данного набора определяются целевым назначением механизма защиты. Необходимо отметить, что механизмы защиты являются сложными сущностями. Каждый механизм защиты может быть осуществлен каким-либо методом,

а каждый метод представляет собой программную или аппаратную реализацию некоторого алгоритма, который обеспечивает конфиденциальность, целостность или доступность. Определим *модель защиты облачного сервиса* как совокупность механизмов защиты, реализованных в рамках конкретной ИС.

Рассмотрим модель ОИС в виде, представленном на рис. 4.

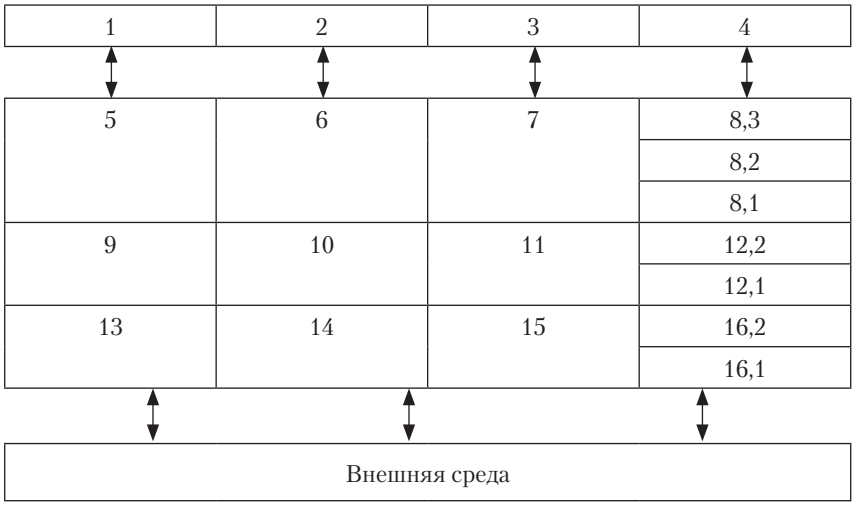

Рис. 4. Упрощенный вид OSE/RM

Для решения задачи построения модели защиты облачного сервиса определим следующие объекты (нумерация соответствует предложенной на рис. 4 модели):

– операции над данными O: $O = \{o_1, o_2, \ldots, o_n\}$, $o_i \in \{1,16\}$;
– бизнес-процесс B: $B = O_i \rightarrow \ldots \rightarrow O_j$, $i, j \in \{1,4\}$;
– механизм защиты Mx: $Mx = \{m_1, m_2, \ldots, m_n\}$, $m_i \in \{1,16\}$;
– облачный сервис S: $S = \mathrm{U}B_i$, $B_i \cap B_j \neq 0$.

Используя введенные определения, можно предложить следующий алгоритм.

Вход: $S = \mathrm{U}B_i$, $B_i \cap B_j \neq 0$, $Mx = 0$.

Шаг 1. Выбрать бизнес-процесс B_1, построить для него $B_1 = O1_i \rightarrow \ldots \rightarrow O1_j$, $i, j \in \{1,4\}$;

Шаг 2. На основе множества, полученного на шаге 1, сформировать множество цепочек вида $O1 = \{o1_1, o1_2, \ldots, o1_n\}$, $o1_i \in \{1,16\}$;

Шаг 3. Сформировать множество механизмов защиты $Mx_1 = \{m1_1, m1_2, ..., m1_n\}$, $m1_i \in \{1,16\}$ для множества цепочек, полученных на шаге 2, причем множество считается окончательно сформированным, если Mx_1 есть биекция $O1$;

Шаг 4. $Mx = Mx \cup Mx_1$, если обработаны все входящие B_i – то выход, иначе, шаг 1;

Выход: Модель защиты ИС $Mx = \cup Mx_i$.

Верификация модели защиты облачной системы.

В качестве иллюстрации продемонстрируем, как алгоритм построения модели защиты ИС может быть использован для выполнения верификации существующей модели защиты для заданного облачного сервиса. Далее автором предлагается модификация алгоритма построения модели защиты с целью выполнения верификации модели защиты облачного сервиса. В алгоритме использованы следующие условные обозначения.

Mx_B – верифицируемая модель защиты, представляет из себя совокупность механизмов защиты.

Алгоритм верификации модели защиты.

Вход: $S = \cup B_i$, $Mx_B = \cup Mx_i$.

Шаг 1. Выбрать бизнес-процесс B_1, построить для него $B_1 = O1_i \rightarrow ... \rightarrow O1_j$, $i, j \in \{1,4\}$;

Шаг 2. На основе множества, полученного на шаге 1, сформировать множество цепочек вида $O1 = \{o1_1, o1_2, ..., o1_n\}$, $o1_i \in \{1,16\}$;

Шаг 3. Сформировать множество механизмов защиты $Mx_1 = \{m1_1, m1_2, ..., m1_n\}$, $m1_i \in \{1,16\}$ для множества цепочек, полученных на шаге 2, причем множество считается окончательно сформированным, если Mx_1 есть биекция $O1$;

Шаг 4. $Mx = Mx \cup Mx_1$, если обработаны все входящие B_i – то выход, иначе, шаг 1;

Выход: Если модель защиты ИС $Mx = \cup Mx_i$, построенная в процессе работы алгоритма, совпадает с верифицируемой моделью защиты ($Mx_B = Mx$), то верифицировать модель защиты, иначе считать верифицируемую модель защиты неоптимальной.

Подход к созданию модели защиты на основе строгого описания защищаемой системы моделью OSE/RM, предложенный в работе, дает ряд преимуществ:

– формируется условный защищаемый периметр, определяемый функционированием бизнес-процессов потребителя облачных услуг;
– обосновывается выбор механизмов защиты и необходимое их количество;
– представляется однозначным образом база, необходимая для проведения верификации модели защиты.

Не теряя основных преимуществ облачных систем, таких как децентрализованность, произвольное изменение топологии и др., можно обеспечить информационную безопасность целевой системы.

Примечания

[1] ISO/IEC TR 14252-96. Information technology. Guide to the POSIX Open System Environment (OSE). 1996.

[2] *Бойченко А.В., Кондратьев В.К., Филинов Е.Н.* Основы открытых информационных систем / Под ред. В.К. Кондратьева. М.: ЕОАИ, 2004.

[3] NIST Cloud Computing Standards Roadmap / National Institute of Standards and Technology, Special Publication 500–291. 2011. July. https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

[4] *Бойченко А.В., Лукинова О.В.* Применение модели POSIX OSE/RM при построении подсистем информационной безопасности // Интеллектуальные системы (AIS'10); Интеллектуальные САПР (CAD-2010): Тр. междунар. науч.-практ. конф. Т. 2. М.: Физматлит, 2010. С. 473–476.

[5] *Кузнецов В.С.* Интерпретация облачных вычислений как открытой информационной системы. Материалы III Всероссийской молодежной конференции по проблемам информационной безопасности «Перспектива 2013». (Таганрог, 9–12 июля 2013 г.). – Таганрог, 2013. С. 171–177.

[6] *Кузнецов В.С., Лукинова О.В.* Представление информационных угроз на основе модели открытой среды // Научно-технический вестник информационных технологий механики и оптики. 2013. № 4 . С. 138–143.

[7] ISO/IEC TR 14252-96.

[8] См. примеч. 2, 4, 6.