7 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 007.51

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ СЕРВИСАХ НА ОСНОВЕ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ

И.А. Зикратов, С.В. Одегов, А.В. Смирных

В работе рассмотрены теоретические аспекты построения защищенных облачных сервисов для обработки информации различной степени конфиденциальности. Предложен новый подход к обоснованию состава средств защиты информации в распределенных вычислительных структурах, заключающийся в представлении задачи оценки рисков как экстремальной задачи принятия решений. Доказывается, что использование метода линейного программирования минимизирует риски информационной безопасности при заданных значениях показателей защищенности с соблюдением экономического баланса на содержание средств защиты и стоимости предоставляемых услуг. Приводится пример, иллюстрирующий полученные теоретические результаты.

Ключевые слова: риски, информационная безопасность, облачные вычисления, целевая функция, угрозы.

Введение

Проблема обеспечения информационной безопасности (ИБ) стоит в ряду первостепенных задач при проектировании информационно-телекоммуникационных систем. Практика показывает, что в настоящее время ядро сетевой архитектуры изменилось с локализованных автономных вычислений на среду распределенных вычислений, что многократно увеличило ее сложность. Широкое распространение получили облачные вычисления – модель обеспечения сетевого доступа к общему пулу ресурсов, которые могут быть оперативно освобождены с минимальными эксплуатационными затратами [1].

Практика показывает, что пользователи облачных технологий передают на аутсорсинг функции хранения и обработки информации различной степени конфиденциальности. В этом случае к поставщику услуг могут предъявляться требования к обеспечению приемлемых уровней рисков ИБ, которые будут зависеть от ценности информационных активов. Следовательно, внедрение облачных технологий формирует актуальную проблему создания методологического подхода для обеспечения ИБ, в частности – снижения рисков ИБ в распределенных системах обработки и хранения данных.

Указанная задача решается путем:

- выявления, анализа и оценки рисков;
- снижения их до приемлемого уровня;
- внедрения адекватных механизмов именно для тех систем и процессов, для которых они необходимы [2].

Выполнение этих этапов позволяет сделать систему безопасности экономически результативной, актуальной и способной реагировать на возникающие угрозы.

Существующие международные стандарты в области менеджмента риска ИБ допускают использование как количественных, так и качественных методов оценки рисков. Наиболее известный вариант решения этой задачи, предлагаемый стандартами, состоит в умножении вероятности реализации угрозы на значение величины ущерба с последующим сопоставлением полученного значения с заданной шкалой [3]. Задача снижения риска в общем виде трактуется как действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском [4].

Таким образом, поставщикам услуг облачных сервисов необходимо, с одной стороны, обеспечить обслуживание существующего потока заявок на обработку информации различной степени конфиденциальности, экономическую результативность облачного сервиса, рациональное распределение ресурсов в облаке, и, с другой стороны, предпринять действия для снижения, а по возможности – минимизации рисков ИБ.

В настоящей работе деятельность по минимизации рисков ИБ в облачных сервисах рассмотрена как решение экстремальной задачи, и предложен метод ее формализации на основе математического аппарата для этого класса задач – линейного программирования (ЛП).

Как известно, ЛП представляет собой набор переменных $\boldsymbol{x} = (x_1, x_2, \ldots x_n)$ и функции этих переменных $f(\boldsymbol{x}) = f(x_1, x_2, \ldots x_n)$, которая носит название ***целевой*** функции [5, 6]. Ставится задача: найти экстремум (максимум или минимум) целевой функции $f(\boldsymbol{x})$ при условии, что переменные $\boldsymbol{x}$ принадлежат некоторой области G:

$$\begin{cases} f(\boldsymbol{x}) => extr \\ \boldsymbol{x} \in G \end{cases}.$$

В зависимости от вида функции $f(\boldsymbol{x})$ и области G различают разделы математического программирования: квадратичное программирование, выпуклое программирование, целочисленное программирование и т.д. ЛП характеризуется тем, что

– функция $f(\boldsymbol{x})$ является линейной функцией переменных $x_1, x_2, \ldots x_n$;
– область G определяется системой линейных равенств или неравенств.

Учитывая особенности метода ЛП, представим формальную постановку задачи для оценки рисков ИБ в облаке, исходя из следующих рассуждений.

Оценка рисков ИБ в облачном сервисе

Пусть в облаке может обрабатываться информация различной степени конфиденциальности $s = 1, 2, ..., M$, где M – количество степеней конфиденциальности информации. Следовательно, облачный сервис должен иметь в своем составе ресурсы различного уровня защищенности, $k = 1, 2, ..., M$. Очевидно, что согласно мандатной модели разграничения доступа при обработке информации s-й степени конфиденциальности на ресурсе k-го уровня защищенности должно выполняться требование

$$s \le k. \quad (1)$$

Для решения задачи квантизации ресурсов облака по уровням защищенности используется подход, представленный в работе [7].

Пусть известны стоимости затрат $C_k^з$ на содержание единицы ресурса различных уровней защищенности $C_1^з, C_2^з, \ldots, C_M^з$, и заданы стоимости обработки единицы информации $C_s^о$ различной степени конфиденциальности $C_1^о, C_2^о, \ldots, C_M^о$. Известен также поток заявок $\boldsymbol{I} = \{I_1, I_2, \ldots, I_s\}$ на обработку информации различной степени конфиденциальности.

Наиболее распространенный способ вычисления риска (R) определяется следующим произведением [4]:

$$R = \sum_i P_i C_i^у ,$$

где P_i – вероятность успешной реализации i-й угрозы; $C_i^у$ – оценка ущерба (стоимости) при успешной реализации i-й угрозы; $i = 1..n$ – количество вероятных угроз.

Введем ограничение. Будем рассматривать систему при наличии одной угрозы. Очевидно, что величину ущерба при реализации угрозы на информацию различной степени конфиденциальности необходимо оценивать дифференцированно. Тогда, зная величины ущерба $C_s^у$ при воздействии угрозы на информацию s-й степени конфиденциальности, и, оценив вероятности реализации угрозы рассматриваемого типа применительно к ресурсу k-го уровня защищенности, построим матрицу рисков $\boldsymbol{r}$:

$$\begin{bmatrix} r_{11} & \cdots & r_{1s} \\ \vdots & \ddots & \vdots \\ r_{k1} & \cdots & r_{ks} \end{bmatrix}, \quad (2)$$

где r_{sk} – риск ИБ при воздействии угрозы на ресурс i-го класса, обрабатывающий информацию j-й степени конфиденциальности.

Требуется определить, сколько единиц ресурсов каждого уровня x_k надо иметь в составе облачного сервиса, чтобы риски ИБ при воздействии заданной угрозы были минимальны. С учетом требования (1) целевая функция принимает следующий вид:

$$x_1 r_{11} + x_2 r_{21} + x_2 r_{22} + x_3 r_{31} + x_3 r_{32} + x_3 r_{33} + .. + x_M r_{MM} \to \min .$$

При этом система ограничений должна обеспечивать выполнение следующих условий:

– обеспечение обслуживания всего потока заявок

$$\sum_i x_i I_i^d \ge \boldsymbol{I},$$

– облачный сервис в искомой конфигурации должен быть экономически рентабелен

$$\sum_i \sum_j x_i C_j^о > \sum_i x_i C_i^з.$$

Последнее ограничение обусловлено тем обстоятельством, что допускается обработка информации низкой степени конфиденциальности на ресурсах высших уровнях защищенности, так, что стоимость обработки для заказчика услуг при этом не должна возрастать. Исходя из этого, для степени конфиденциальности $s = i$, при обработке на ресурсе уровня $k = j$ (j>i), стоимость обработки должна быть равной $C_i^о$. Очевидно, система ограничений должна быть дополнена требованиями целостности и не отрицательности величин, исходя из их физического смысла.

Таким образом, в рамках предлагаемого подхода должны быть решены следующие задачи:

– квантизация ресурсов облачного сервиса по уровням защищенности;
– идентификация уязвимостей и угроз;
– классификация обрабатываемой информации по степеням конфиденциальности;
– количественная оценка вероятности реализации угрозы и влияние на состояние облачного сервиса потенциальных угроз;
– определение экономического баланса между затратами на содержание системы защиты информации (СЗИ) ресурса облачного сервиса и предоставляемой стоимостью услуг.

Пример оценки рисков ИБ при использовании ЛП

Проиллюстрируем полученный результат тривиальным примером. На рисунке представлен фрагмент распределенной автоматизированной системы в составе которой имеются ресурсы различной степени защищенности – группы *A*, *B* и *C*, в зависимости от СЗИ, реализованной на данном ресурсе:

– 1-я группа (*A*) – ресурсы с низким уровнем защищенности;
– 2-я группа (*B*) – ресурсы с высоким уровнем защищенности;
– 3-я группа (*C*) – защищенные ресурсы.

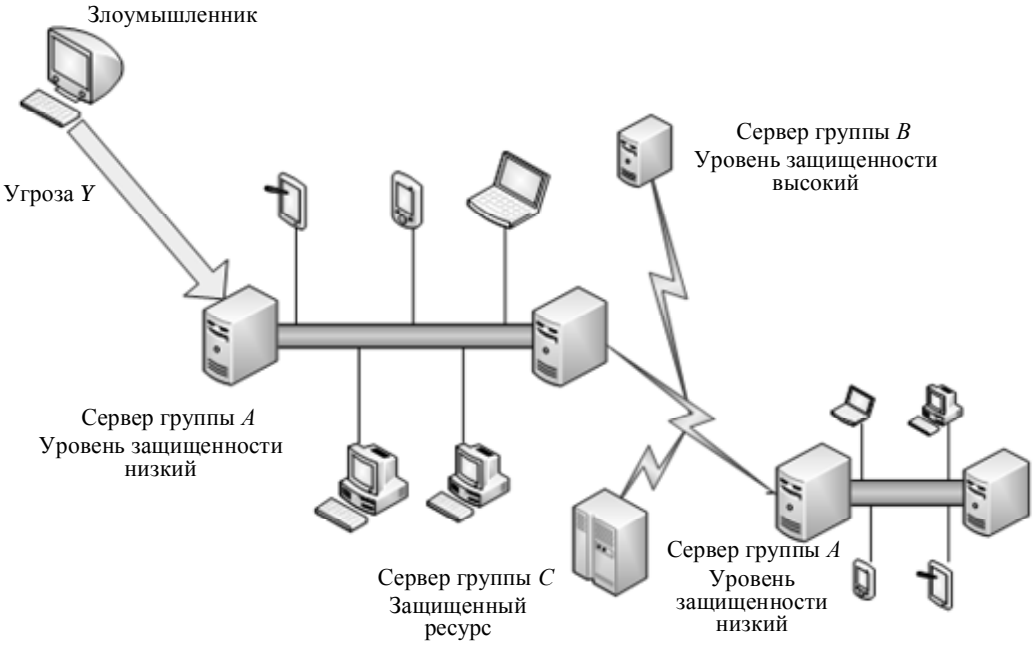

Рисунок. Фрагмент распределенной автоматизированной системы

Стоимость затрат на содержание единицы ресурса *n*-ой группы: $A = 1$, $B = 3$, $C = 8$ условных единиц. Пусть в рассматриваемой системе обрабатывается информация различных категорий конфиденциальности l_s ($s = 1, 2, 3$):

– l_1 – открытая информация;
– l_2 – конфиденциальная информация;
– l_3 – критически важная информация.

Согласно неравенству (1), информация категории l_1 обрабатывается на ресурсах любой группы, информация категории l_2 может обрабатываться на ресурсах групп B и C. Информация категории l_3 обрабатывается только на ресурсах группы C. Стоимость обработки единицы информации *s*-ой степени конфиденциальности составляет $l_1 = 2$, $l_2 = 5$ и $l_3 = 10$.

Масштабирование ресурсов, требуемых для обработки информации *s*-ой степени конфиденциальности осуществляется при помощи заявок $\boldsymbol{I}$. Поток заявок составляет не менее: $I_1 = 200$; $I_2 = 80$; $I_3 = 40$ единиц.

Пусть из общей статистики угроз вида Y известна вероятность реализации угрозы P_i для каждого типа ресурсов P_A, P_B и P_C. Очевидно, что P_i реализации угрозы зависит от уровня защищенности ресурса, но не зависит от степени конфиденциальности информации *s*, обрабатываемой на ресурсе. Составим матрицу рисков (2). Пусть значения вероятности P_i и уровня ущерба $C_s^{\text{у}}$ для различных групп ресурсов и степеней конфиденциальности защищаемой информации: $P_A = 1$, $P_B = 0{,}5$ и $P_C = 0{,}1$ и $C_1^{\text{у}} = 2$, $C_2^{\text{у}} = 5$ и $C_3^{\text{у}} = 10$. Тогда элементы матрицы рисков r_{is} будут иметь значения, представленные в таблице.

Проведем расчет количества емкости заявок I_n. На ресурсах группы A могут обрабатываться категории информации $I_1 = 200$; на ресурсах группы B обрабатываются заявки I_1 и $I_2 = 280$ и на ресурсах группы C могут обрабатываться только заявки категории $I_3 = 80$. Общее количество заявок I_n составляет 320. Решение задачи симплекс-методом дает следующий результат:

– количество единиц ресурса группы A $x_1 = 40$ единиц;
– для группы B $x_2 = 180$ единиц;
– для группы C $x_3 = 100$ единиц.

Анализ результатов показывает, что полученное решение:

– содержит однозначно трактуемые количественные оценки состава ресурсов, различной степени защищенности в облачном сервисе;
– обеспечивает поток заявок на обработку информации различной степени конфиденциальности;
– не противоречит известным моделям разграничения доступа.

	Открытая информация (l_1)	**Конфиденциальная информация (l_2)**	**Критическая информация (l_3)**
Ресурс группы *A*	2	5	10
Ресурс группы *B*	5	2,5	5
Ресурс группы *C*	0,2	0,5	1

Таблица. Матрица рисков ИБ

При этом обеспечивается минимизация рисков ИБ для заданных показателей защищенности и матрицы потерь при соблюдении экономического баланса на содержание СЗИ и стоимости предоставляемых услуг на обработку конфиденциальной информации.

Заключение

Широкое распространение облачных вычислений на рынке поставщиков IT-услуг приводит к необходимости совершенствования научно-методического аппарата для построения систем защиты информации. В работе впервые предложен метод для количественного обоснования состава ресурсов различного уровня защищенности в облачном сервисе. Предлагаемый новый подход позволяет поставщику услуг на основе матрицы рисков, требований заказчиков к обеспечению конфиденциальности, целостности и доступности информации, соблюдения экономических интересов осуществлять оценку и минимизацию рисков информационной безопасности в облачных сервисах. Выполнив подобные расчеты для всех видов угроз безопасности в соответствии с моделью угроз можно принимать обоснованные решения для конфигурации емкости облачных сервисов и ресурсов различного уровня защищенности.

Применимость методики обусловлена использованием апробированного математического аппарата, непротиворечивостью полученных результатов, а также отражает требования международных стандартов в области оценки рисков. Кроме того, разработанный метод оценки рисков соответствует основным постулатам мандатной модели разграничения доступа.

Дальнейшим направлением научной работы являются:

1. оценка чувствительности полученных результатов, так как известным недостатком линейного программирования является высокая чувствительность к изменению исходных данных;
2. возможность адаптации предложенного метода к ролевой модели разграничения доступа, как наиболее распространенной в облачных сервисах.

Литература

1. Jansen W., Grance T. Guidelines on Security and Privacy in Public Cloud Computing. Draft NIST Special Publication 800-144. – Gaithersburg, 2011. – 52 p.
2. Catteddu D., Hogben G. Cloud Computing: Benefits, risks and recommendations for information security. – Heraklion: ENISA, 2009. – 125 p.
3. Марков А., Цирлов В. Управление рисками – нормативный вакуум информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.osp.ru/os/2007/08/4492873/, свободный. Яз. рус. (дата обращения 30.11.2012).
4. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Введ. 30.11.2010. – М.: Стандартинформ, 2011. – 51 с.
5. Хемди А. Таха. Введение в исследование операций. – М.: Вильямс, 2007. – 912 с.
6. Вентцель Е.С. Введение в исследование операций. – М.: Советское радио, 1964 – 391 с.
7. Зикратов И.А., Одегов С.В. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 121–126.

Зикратов Игорь Алексеевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, доцент, зав. кафедрой, zikratov@cit.ifmo.ru

Одегов Степан Викторович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, odegov.sv@gmail.com

Смирных Александр Валентинович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, ст. преподаватель, smirnykh_av@spb.power-m.ru