МЕТОД ОБРАБОТКИ ИНФОРМАЦИИ ДЛЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В УПРАВЛЕНИИ ОБЛАЧНЫМ СЕРВИСОМ

Ряполова Е.И.[1], Шрейдер М.Ю.[2], Боровский А.С.[3]

Цель статьи *заключается в разработке метода обработки информации на основе использования известного экспертно-аналитического подхода анализа иерархий Т. Саати для поддержки принятия решений в задаче определения уровня текущей защищенности элементов облачного сервиса.*

Метод исследования и разработки: *основан на использовании теории множеств, а именно на представлении модели обеспечения безопасности облачного сервиса в виде четких соответствий четких множеств. Метод включает: построение модели управления безопасностью облачного сервиса на основе четких соответствий четких множеств. Модель представлена объединением четырех множеств: множество нарушителей в облачном сервисе, множество доступов к облачному сервису, множество элементов облачного сервиса, множество технических и программных средств защиты облачного сервиса. Соответствия между представленными множествами модели безопасности облачного сервиса определяются экспертно-аналитическим путем метода анализа иерархий Т. Саати.*

Полученные результаты: *предложена модель функционирования системы безопасности облачного сервиса в виде взаимодействия множеств, которая позволяет определить состав комплекса аппаратно-программных средств защиты, основываясь на экспертных знаниях. Соответственно, такой способ моделирования способствует определению варианта системы безопасности облачного сервиса с целью выбора наилучшей стратегии его защиты. Полученные в модели коэффициенты соответствия множеств модели системы безопасности облачного сервиса показывают уровень необходимости наличия того или иного средства защиты от определенной угрозы, в совокупности определяя желаемый состав его системы защиты.*

Ключевые слова: *системы безопасности, аппаратные средства защиты, программные средства защиты, облачные вычисления, четкие множества, четкие соответствия, теория множеств, композиция соответствий, метод анализа иерархий.*

DOI:10.21681/2311-3456-2018-3-39-46

Введение

В настоящее время облачные технологии интенсивно развиваются и внедряются на предприятия [1]. Технология облачных вычислений направлена на предоставление широкого спектра сервисов и ресурсов для облачных пользователей, что обеспечивает массовость и публичность системы облачных вычислений. Среди множества пользователей могут оказаться и нарушители, что может привести к несанкционированному доступу к облачному сервису [2-8].

Для поддержки принятия решений в процессе управления облачным сервисом необходимо разработать математическую модель, учитывающую высокую степень неопределенности, с минимумом входных данных. Теоретической основой представления данной модели составляют теория множеств и метод анализа иерархий Т.Саати.

Основная часть

В обобщенной схеме процесса обеспечения безопасности облачного сервиса можно выделить несколько множеств в независимости от того, какие ресурсы предоставляют облачные платформы (рисунок 1) [9-14]:

– множество угроз, реализуемых в облаке X={xi | i=1,N}. Под угрозой можно понимать намерение нарушителя нанести физический, материальный или иной вред, понесший за собой нарушение целостности и конфиденциальности информации. Например: искажение информации, несанкционированный доступ к информации, хищение информации и др.

Каждая угроза может характеризоваться: $P_{угр}$ – вероятностью появления и реализации i-ой угрозы; $C_{угр}$ – значимостью при нанесении ущерба;

– множество средств защиты в предоставляемом облачном сервисе Z={zk | k=1,M}, которые выполняют функции обнаружения и блокировки угрозы безопасности облачной платформы. Установленные средства защиты характеризуются A_iA_i – способностью противодействовать реализации угрозы, эту функцию в облачных вычислениях выполняет агент безопасности, отвечающий за мониторинг и адекватность запросов пользователей в системе об-

1. Ряполова Елена Ивановна, кандидат педагогических наук, доцент, доцент кафедры «Вычислительная техника и защита информации», ФГБОУ ВО «Оренбургский государственный университет», Оренбург, Россия, e-mail: ananeva_ei@mail.ru
2. Шрейдер Марина Юрьевна, кандидат технических наук, доцент кафедры «Управление и информатика в технических системах», ФГБОУ ВО «Оренбургский государственный университет», Оренбург, Россия, e-mail: marshr@mail.ru
3. Боровский Александр Сергеевич, доктор технических наук, доцент, заведующий кафедрой «Управление и информатика в технических системах», ФГБОУ ВО «Оренбургский государственный университет», Оренбург, Россия, e-mail: borovski@mail.ru

Рисунок 1 – Обобщенная схема процесса обеспечения безопасности облачного сервиса

лачных вычислений, предоставляет возможные варианты запросов в случае неверно выбранных действий или попытки несанкционированного доступа к ресурсам системы облачных вычислений, так же отвечает за безопасное взаимодействие системы в целом;

– облачный сервис представляет собой множество Y = {yj | j=1,L} с рядом предоставляемых сервисов. Множество характеризуется показателями: $P_{защ}$– коэффициент надежности предоставляемого сервиса или ресурса, $V_{сер}$– ценность предоставляемого сервиса, $H_{рес}$–коэффициент надежности (безотказной работы) аппаратных ресурсов для предоставления сервисов, $S_{рес}$–коэффициент надежности (безотказной работы) программных ресурсов для предоставления облачных сервисов.

– множество пользователей облачных сервисов P = {pj | j=1,K} (внутренние, внешние пользователи сервиса).

– множество потоков информации P(N,L), PL={PLj | j=1,M},

PN= {PNj | j=1,K}(PL – безопасные потоки,PN – потенциально опасные потоки информации, несущие различного вида угрозы безопасности).

– множество доступа R={rj | j=1,N}(содержит монитор безопасности), отвечает за персонофицируемость пользователей, аутентификацию и идентификацию пользователей, осуществляет управление доступом и контроль доступа к сервисам с учетом разработанной политики безопасности.

Процесс обеспечения безопасности облачно сервиса включает следующие операции:

– пользователи облачного сервиса P отправляют запрос на предоставление доступа к ресурсам облачного сервиса, при этом запрос проходит ряд этапов проверки, прежде чем пользователь получит доступ к ресурсам облака;

– запрос пользователя поступает во множество потоков информации P (N, L), где в свою очередь генерируются два вида потоков PL – безопасные потоки, PN – потенциально опасные потоки информации, несущие различного вида угрозы безопасности, далее запрос поступает во множество доступа R, данное множество отвечает за проверку запроса и предоставление доступа пользователю;

– при проверке определяется уровень секретности запрашиваемого ресурса сервиса (каждому уровню секретности ставится в соответствие метка доступа, уровень имеет большую степень секретности, если значение его метки доступа меньше) и права доступа данного пользователя к сервису (совокупность правил, регламентирующих порядок и условия доступа облачного пользователя к облачному сервису);

– множество средств защиты Z так же проверяет запрос на возможную угрозу безопасности облачного сервиса.

Возможен обход множества доступа, что повлечет за собой увеличение вероятности реализации угрозы нарушителем, но в системе безопасности облачного сервиса предусмотрено множество средств защиты, которое так же направлено на проверку запроса пользователя. Обход множества средств защиты так же возможен. В случае данного вида обхода, в облачном сервисе предусмотрен агент безопасности, отвечающий за безопасное взаимодействие всех компонентов облачного сервиса.

Модель функционирования системы обеспечения безопасности облачного сервиса (рисунок 2) включает в себя пять основных множеств они описаны выше и четыре дополнительных:

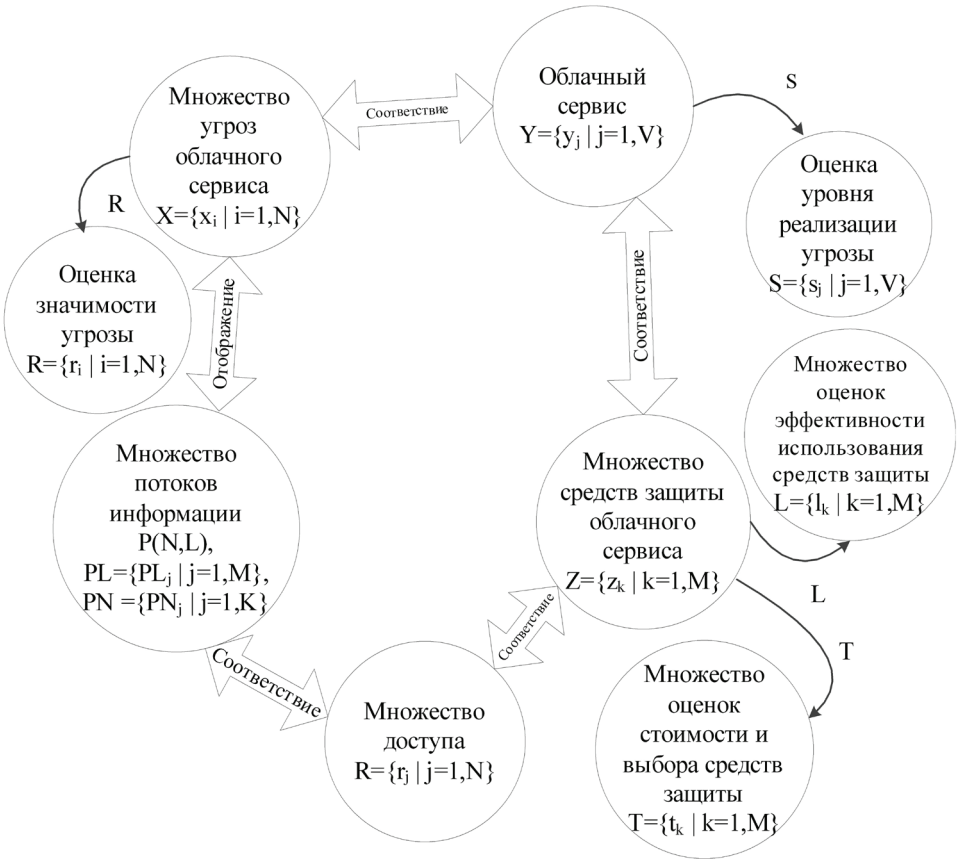

Рисунок 2 - Схема модели функционирования системы безопасности облачного сервиса на основе четких множеств

1) Множество оценок значимости угрозы R={ri | i=1,N}. В данном случае под «значимостью» понимают риск реализации той или иной угрозы для облачного сервиса.

2) Множество оценок уровня реализации угрозы S={sj | j=1,V}. Под «реализацией» в данном случае понимают оценку ущерба от реализации угрозы на yj облачный сервис.

3) Множество оценок эффективности использования средств защиты L={lk | k=1,M}. Здесь под «эффективностью» понимают степень выполнения zk функций средством защиты в облачном сервисе.

4) Множество оценок стоимости и выбора средств защиты T={tk | k=1,M}. Под «стоимостью» понимаются финансовые затраты на приобретение, использование и сопровождение zk средства защиты облачного сервиса.

Используя математический аппарат теории множеств, установим соответствия между основными множествами:

– соответствие множества потоков информации P(N,L) множеству доступов представляется в виде множества $Q \subseteq P(N,L) \times R$, устанавливающее взаимосвязь, которая указывает: возможность получения доступа к облачным сервисам. Для каждого потока информации необходимо определить qki – оценку возможности получения доступа к облачным сервисам;

– соответствие множества доступов R={rj | j=1,N} множеству средств защиты облачного сервиса Z={zk | k=1,M} представляется в виде множества $W \subseteq R \times Z$, устанавливающее взаимосвязь уровня противодействия потоку информации средствами защиты облачного сервиса. Для одного средства защиты будут определены N коэффициентов соответствия wki (i=1,N) – оценок уровня противодействия (блокирования угрозы) i – ой угрозе;

– композиция соответствий множества потоков информации P(N,L) множеству доступов R и множества доступов R множеству средств защиты облачного сервиса Z будет иметь вид: $q(w)=(P(N,L), Z, Q \circ W)$, $Q \circ W \subseteq P(N,L) \times Z$ – есть распределение средств защиты на множество информационных потоков;

– соответствие множества потоков информации P(N,L) множеству элементов облачного сервиса Y, представляется в виде множества $G \subseteq P(N,L) \times Y$, устанавливающее взаимосвязь, которая указывает: насколько потоки информации, в частности каждый вид угрозы в потоке PN вероятен для каждого элемента облачного сервиса. Для одной угрозы в потоке информации PN будет определен V коэффициент соответствия gij (j=1, V) – оценок вероятности реализации i – ой угрозы в потоке PN по отношению к j–му элементу облачного сервиса;

– итоговая композиция соответствий множеств модели будет иметь вид $(Q \circ W) \circ G \subseteq Z \times Y$ устанавливающая взаимосвязь, которая указывает: какие средства защиты более эффективны для защиты того или иного элемента облачного сервиса в зависимости от вида угрозы в потоке PN.

Все соответствия и отображения, используемые в модели, определяются экспертно-аналитическим путем метода анализа иерархий Т. Саати. При использовании этого метода проводятся парные сравнения элементов по отношению к их воздействию на общую для них характеристику.

Используемая шкала оценок метода анализа иерархий приведена в таблице 1.

Для поддержки принятия решений по выбору средств защиты в процессе функционирования облачного сервиса экспертные знания применяем для определения: qki – оценок возможности получения доступа i -го потока информации к облачному сервису; оценок уровня противодействия угрозе – wki, оценок вероятности реализации i – ой угрозы в потоке информации по отношению к j–му элементу облачного сервиса gij , оценок уровня реализации угрозы – sj , оценок эффективности использования средства защиты – lk .

Таблица 1 – Шкала экспертных оценок в методе анализа иерархий

Шкала интенсивности	Качественные суждения
1	равная важность
3	умеренное превосходство одного над другим
5	существенное превосходство одного над другим
7	значительное превосходство одного над другим
9	очень сильное превосходство одного над другим
2, 4, 6, 8	соответствующие промежуточные значения

Рассмотрим условный пример применения средств защиты в процессе функционирования облачного сервиса.

Множества модели системы управления безопасностью облачного сервиса содержат следующие элементы:

1) Множество потоков информации: PN(x1) – потоки информации от внутреннего нарушителя непреднамеренно пытающегося совершить злоумышленные действия в облачном сервисе;

PN(x2) – потоки информации от внешнего нарушителя непреднамеренно (случайно, без заранее обдуманного намерения) пытающегося совершить злоумышленные действия в облачном сервисе;

PN(x3) – потоки информации от внешнего нарушителя преднамеренно пытающегося совершить злоумышленные действия в облачном сервисе;

PN(x4) – потоки информации от внутреннего нарушителя преднамеренно пытающегося совершить злоумышленные действия в облачном сервисе.

2) Множество доступов: r1 – права доступа, r2–уровень секретности, то есть категория секретности информации с определенными правами доступа к ней.

3) Множество элементов облачного сервиса: y1–система виртуализации; y2–система управления вычислительными ресурсами; y3–хранилище образов виртуальных машин; y4–хранилище данных; y5–система авторизации и аутентификации, y6–веб интерфейс.

4) Множество средств защиты облачного сервиса: z1 – средства обнаружения информационного потока от нарушителя в облачном сервисе; z2 – средства контроля доступа информационного потока от нарушителя в облачный сервис; z3 – средства блокирования информационного потока от нарушителя.

Находим оценки уровня доступа к сервису i-го потока информации – коэффициенты соответствия q11, q21, q31, q41,. Матрица парных сравнений представлена в таблице 2. Матрицы составляются для каждого типа доступа к облачному сервису.

Таблица 2 – Матрица парных сравнений для определения оценок уровня доступа к сервису i-го потока информации

r1	PN(x1)	PN(x2)	PN(x3)	PN(x4)
PN(x1)	1	1\2	5	7
PN(x2)	2	1	7	9
PN(x3)	1\5	1\7	1	7
PN(x4)	1\	1\9	1\7	1

Коэффициенты определяются вычислением вектора приоритетов, по матрице парных сравнений следующим способом: суммировать элементы каждой строки и нормализовать делением каждой суммы на сумму всех элементов. Первый элемент результирующего вектора будет приоритетом первого объекта, второй – второго и т. д.

В результате получаем оценки:
q1 1 = (1+1/2+5+7)/42,23 = 0,32;
q2 1 = (2+1+7+9)/42,23 = 0,45;
q3 1 = (1/5+1/7+1+7)/42,23 = 0,2;
q4 1 = (1/7+1/9+1/7+1)/42,23 = 0,03;

Аналогично вычисляются: оценки уровня доступа к сервису i-го потока информации для всех доступов – коэффициенты qji (результаты представлены в таблице 3).

Таблица 3 – Оценки уровня доступа к сервису i-го потока информации для всех доступов

вероятности реализации	r1	r2
PN(x1)	0,32	0,29
PN(x2)	0,45	0,46
PN(x3)	0,19	0,2
PN(x4)	0,03	0,04

Далее находим оценки уровня противодействия (блокирования угрозы) i – ой угрозе – wki. Коэффициенты соответствия представлены в таблице 4.

Таблица 4 – Матрица парных сравнений для определения оценки уровня противодействия (блокирования угрозы) i – ой угрозе

PN(x1)	z1	z2	z3
z1	1	1/3	1/3
z2	3	1	1/5
z3	3	5	1

Полученные коэффициенты для всех видов угроз представлены в таблице 5.

Таблица 5 – Оценки уровня противодействия (блокирования угрозы) i – ой угрозе

Уровень противодействия	PN(x1)	PN(x2)	PN(x3)	PN(x4)
z1	0,11	0,1	0,15	0,12
z2	0,32	0,31	0,29	0,3
z3	0,56	0,6	0,55	0,57

Далее находим оценки вероятности реализации i – ой угрозы в потоке информации по отношению к j–му элементу облачного сервиса – gij. Матрица парных сравнений для первого элемента облачного сервиса представлена в таблице 6.

Таблица 6 – Матрица парных сравнений для определения оценок вероятности реализации i – ой угрозы в потоке информации по отношению к j–му элементу облачного сервиса

y1	PN(x1)	PN(x2)	PN(x3)	PN(x4)
PN(x1)	1	1/7	3	1/9
PN(x2)	7	1	7	9
PN(x3)	1\3	1\7	1	7
PN(x4)	9	1\9	1\7	1

Полученные оценки вероятности реализации угроз на элементы облачного сервиса представлены в таблице 7.

Таблица 7 – Оценки вероятности реализации угроз на элементы облачного сервиса

вероятности реализации угрозы	y1	y2	y3	y4	y5	y6
PN(x1)	0,09	0,05	0,1	0,16	0,13	0,22
PN(x2)	0,52	0,1	0,4	0,25	0,15	0,45
PN(x3)	0,18	0,34	0,2	0,31	0,25	0,13
PN(x4)	0,21	0,51	0,3	0,27	0,46	0,2

В примере взяты два вида оценок из четырех, представленных в модели. Для определения оценок уровня реализации угрозы – sj, оценок эффективности использования средства защиты – lk используются матрицы парных сравнений в таблицах 8, 9.

Таблица 8 – Матрица парных сравнений для определения оценок уровня реализации угрозы

уровни реализации угрозы	y1	y2	y3	y4	y5	y6
y1 – система виртуализации	1	1/3	1/3	1/9	1/7	5
y2 – система управления вычислительными ресурсами	3	1	5	1	2	7
y3 – хранилище образов виртуальных машин	3	1/5	1	1/7	1/3	9
y4 – хранилище данных	9	1	7	1	1/3	9
y5 – система авторизации и аутентификации	7	1/2	3	3	1	7
y6 – веб интерфейс	1/5	1/7	1/9	1/9	1/7	1

Таблица 9 – Матрица парных сравнений для определения относительной эффективности использования средств защиты облачного сервиса

Относительная эффективность	z1 (средства обнаружения информационного потока)	z2 (средства контроля доступа информационного потока)	z3 (средства блокирования информационного потока)
z1	1	1/3	1/5
z2	3	1	1/2
z3	5	2	1

Используя полученные данные в таблицах 8, 9 вычисляем следующие коэффициенты:

sj – относительный уровень реализации угроз в отношении элемента облачного сервиса: система виртуализации – 0,076; система управления вычислительными ресурсами – 0,21; хранилище образов виртуальных машин -0,15; хранилище данных– 0,3; система авторизации и аутентификации – 0,24, веб интерфейс – 0,02.

lk – относительная эффективность использования средства защиты облачного сервиса: средства обнаружения информационного потока от нарушителя в облачном сервисе – 0,11; средства контроля доступа информационного потока от нарушителя в облачный сервис – 0,32; средства блокирования информационного потока от нарушителя – 0,57.

Согласно методу Саати для получения общей оценки каждого объекта, нужно умножить вес оценки этого объекта по некоторому критерию на вес этого критерия.

По полученным коэффициентам соответствия: qki, wki рассчитываем следующие оценки:

– gij – оценка вероятности появления и реализации угрозы от каждого потока информации с учетом реализации угрозы в отношении элемента облачного сервиса, расчитывется gi j = qki · sj , где i – номер угрозы, j – номер зоны объекта;

– hk i – оценка уровня противодействия каждого средства защиты облачного сервиса по отношению ко всем видам угроз с учетом оценок эффективности средств, расчитывается hk i = wki· lk, где k – номер средства охраны, i – номер угрозы.

Коэффициенты gij, hk i отображены в таблицах 10, 11.

Таблица 10 – Оценки вероятности появления и реализации угрозы от каждого потока информации в зависимости с учетом реализации угрозы в отношении элемента облачного сервиса

вероятности реализации угрозы	y1	y2	y3	y4	y5	y6
PN(x1)	0,00684	0,0105	0,015	0,0384	0,0312	0,0044
PN(x2)	0,03952	0,0210	0,060	0,0750	0,0360	0,0090
PN(x3)	0,01368	0,0714	0,030	0,0930	0,0600	0,0026
PN(x4)	0,01596	0,1071	0,045	0,0810	0,1104	0,0040

Таблица 11 – Оценки уровня противодействия каждого средства защиты облачного сервиса по отношению ко всем видам угроз с учетом оценок эффективности средств защиты

Уровень противодействия	PN(x1)	PN(x2)	PN(x3)	PN(x4)
z1	0,0121	0,011	0,0165	0,0132
z2	0,1024	0,0992	0,0928	0,0960
z3	0,3192	0,3420	0,3135	0,3249

Далее проводится расчет композиции соответствий множества средств защиты множеству элементов облачного сервиса (таблица 12). Произведение матриц осуществляется по формуле: $f_{kj} = \sum_{i=1,N} (g_{ij} \times h_{ki})$

Таблица 12 – Соответствие средств защиты элементам облачного сервиса

	y_1	y_2	y_3	y_4	y_5	y_6
z1	0,00095	0,00294	0,00019	0,00389	0,00032	0,00024
z2	0,00742	0,02006	0,01459	0,02777	0,02293	0,00221
z3	0,02417	0,08847	0,04933	0,20354	0,07695	0,00659

По полученным оценкам осуществляется принятие решения по выбору средств защиты для элемента облачного сервиса. Чем выше оценка, тем больше эффективность применения данного средства защиты [15-20].

Выводы:

1. Предложена обобщенная схема процесса обеспечения безопасности облачного сервиса. На схеме показан процесс взаимодействия выделенных множеств с потоками информации от каждого множества, схема дает четкое понимание взаимосвязи множества пользователей и облачного сервиса с возможностью обхода различного рода средств защиты облачного сервиса. Понимание процесса обеспечения безопасности облачного сервиса способствует построению дальнейшей стратегии управления облачным сервисом и обеспечения его безопасности.

2. Разработана модель функционирования системы обеспечения безопасности облачного сервиса. Данная модель показывает непрерывные процессы преобразования и обмена информацией с целью автоматизации процесса поиска угроз в облачном сервисе. В нее входят пять основных множеств: множество угроз; модель облачного сервиса, представлена в виде двух множеств: программная часть и аппаратная часть облачного сервиса, множество средств защиты облачного сервиса, множество доступа, множество потоков информации и четыре дополнительных множества: множество оценок значимости угроз облачного сервиса, множество оценок реализации угроз, множество оценок эффективности использования средств защиты, множество оценок стоимости и выбора средств защиты облачного сервиса. Данная модель может использоваться в дальнейшем для принятия решений в процессе управления облачным сервисом.

3. Рассмотрен условный пример расчета модели в задаче выбора средств защиты в процессе функционирования облачного сервиса. Множества модели системы управления безопасностью облачного сервиса содержат следующие элементы: множество потоков информации, множество доступов, множество элементов облачного сервиса, множество средств защиты облачного сервиса. Метод включает расчет следующих коэффициентов и оценок: относительного уровня реализации угроз в отношении элемента облачного сервиса, относительной эффективности использования средства защиты облачного сервиса, оценки вероятности появления и реализации угрозы от каждого потока информации с учетом реализации угрозы в отношении элемента облачного сервиса, оценки уровня противодействия каждого средства защиты облачного сервиса по отношению ко всем видам угроз с учетом оценок эффективности средств. Принятия решений по применению имеющихся средств защиты осуществляется на основе полученных итоговых оценок. Применение данного метода позволит использовать наиболее эффективные средства защиты по отношению к каждому элементу облачного сервиса.

Рецензент: *Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры ИУ-8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, г. Москва, Россия. E-mail: v.tsirlov@bmstu.ru*

Литература

1. Фролов А.Л., Подлевских А.П. Оценка эффективности внедрения в деятельность организации облачных технологий на основе упрощенной методики расчета совокупной стоимости владения // Фундаментальные исследования. 2015. № 11(часть 5). С. 1048-1053.
2. Никольский, Алексей Валерьевич. Защита облачных вычислений от атак на средства виртуализации: диссертация ... кандидата технических наук: 05.13.19 / Никольский Алексей Валерьевич; [Место защиты: С.-Петерб. гос. политехн. ун-т].– Санкт-Петербург, 2013.– 148 с.
3. Пескова О.Ю., Степовая К.Е. Безопасность контроля доступа к облачным системам // Информационное противодействие угрозам терроризма. 2014. № 23. С.110-120.
4. Шпаков Д.В. Изучение проблемы безопасности облачных технологий // Журнал гуманитарных наук. 2017. № 1(17). С.162-166.
5. Пескова О.Ю., Степовая К.Е. Обобщенные требования по обеспечению безопасности облачных сервисов // Информационное противодействие угрозам терроризма. 2014. № 23. С.120-130.
6. Зубарев И.В., Радин П.К. Основные угрозы безопасности информации в виртуальных средах и облачных платформах // Вопросы кибербезопасности. 2014. № 2(3). С. 40 – 45.
7. Зорин Е.Л., Чичварин Н.В. Информационная безопасность САПР/PLM , применяющих облачные технологии // Вопросы кибербезопасности. 2014. № 4(7). С. 23 – 29.
8. Глинская Е.В., Чичварин Н.В. Информационная безопасность открытых каналов передачи проектной документации, продуцируемой в САПР // Вопросы кибербезопасности. 2014. № 4(7) . С. 11 – 22.
9. Боровский А.С. Интегрированный подход к построению систем физической защиты объектов // Наука и образование транспорту. 2016. №2. С. 12-16.
10. Боровский А.С. Программный комплекс оценки инженерно-технической защищенности потенциально опасных объектов // Программные продукты и системы. 2014. №3(107). С.141 – 147.
11. Боровский А.С. Обобщенная модель системы физической защиты как объект автоматизированного проектирования // Вестник компьютерных и информационных технологий. 2014. №10. С.45 – 52.
12. Боровский А.С. Метод определения оптимального уровня возможностей средств инженерно-технической защиты объекта в задачах проектирования систем физической защиты // Информационные технологии. 2014.№12.С.67 – 75.
13. Костин В.Н., Боровский А.С. Метод оценки утечки конфиденциальной информации о функционировании системы защиты объекта информатизации по информационному критерию // Вестник компьютерных и информационных технологий. 2016. №8. С.34 – 43.
14. Боровский А.С., Тарасов А.Д. Программный комплекс информационной поддержки решения задачи проектирования системы физической защиты // Системы управления и информационные технологии. 2016. № 4.1(66). С. 122-128
15. Шидловский, В.В. Информационная модель как основа системы поддержки принятия решений / В.В.Шидловский [и др.] // Информационные технологии в проектировании и производстве. 2015. № 1 (157). С. 14–21.
16. Мелихова, О.А. Обзор моделей систем принятия решений / О.А.Мелихова, Э.Г.Руденко, О.А.Логинов // Актуальные проблемы гуманитарных и естественных наук. 2015. № 6–1. С. 78 – 83.
17. Вяткин, А.Ю. Системы поддержки принятия решений – современный этап развития информационных систем / А.Ю.Вяткин, Д.В.Смирнов, И.А.Кочетов // Известия Института инженерной физики. 2015. Т. 1. № 35. С. 40 – 42.
18. Витенбург Е.А. Формализованная модель системы интеллектуальной поддержки принятия решений в области защиты информации // Известия тульского государственного университета. Технические науки. 2017. № 7. С. 268 – 274.
19. Ломазов В.А., Гостищева Т.В., Климова Н.А. Нечеткий анализ угроз и выбор вариантов системы информационной безопасности инновационного проекта // Современные наукоемкие технологии. 2017. № 10. С. 26 – 31.
20. Витенбург Е.А., Никишова А.В., Чурилина А.Е. Системы поддержки принятия решений в информационной безопасности // Вестник компьютерных и информационных технологий. 2015. № 4(130). С. 50 – 56.

THE METHOD OF INFORMATION PROCESSING FOR DECISION SUPPORT IN THE MANAGEMENT OF CLOUD SERVICES

Ryapolova E.I.[4], Schreider M.Y.[5], Borovski A.S.[6]

4. Elena Ryapolova PhD, Assistant Proffesor of the Department "Computer engineering and information protection", Federal State-Funded Educational Institution of Higher Education "Orenburg state University", Orenburg, Russia. E-mail: ananeva_ei@mail.ru
5. Marina Shreider, PhD, Assistant Proffesor of the Department " Management and Informatics in technical systems", Federal State-Funded Educational Institution of Higher Education "Orenburg state University", Orenburg, Russia. E-mail: marshr@mail.ru
6. Alexandr Borovski, Dr.Sc., Head of the Department "Management and Informatics in technical systems", Federal State-Funded Educational Institution of Higher Education "Orenburg state University", Orenburg, Russia.
E-mail: borovski@mail.ru

Abstract. *The purpose of the article is the information processing method which based on the using of the well-known expert-analytical approach of the analysis of the hierarchies of T. Saati to support decision-making in the task of determining the level of current security of the cloud service elements. The scientific research and method based on the using of set theory, namely the representation of the model of cloud service security in the form of clear correspondences of clear sets. The method includes: building a model of cloud service security management on the bases of clear correspondences of clear sets. The model is represented by a combination of four scores: scores of violators in the cloud service, scores of access to the cloud service, scores of elements of the cloud service, scores of hardware and software protection of the cloud service. The correspondence between the presented sets of the cloud service security model is determined by the expert-analytical method of the analysis of T. Saati hierarchies. Results: the model of the functioning of the security system of cloud service is proposed in the form of interaction of sets, which allows identify the composition of the complex hardware and software protection based on the expert knowledge. Accordingly, this method of modeling helps to determine the security option of the cloud service in order to choose the best strategy for its protection. The coefficients of correspondence of sets of the cloud service security system model, which are obtained in the model show the level of need for this or that means of protection against a certain threat, determining the desired composition of its security system together.*

Keywords: *security systems, hardware protection, software protection, cloud computing, clear sets, clear correspondence, set theory, composition of correspondences, method of analysis of hierarchies.*

References

1 Frolov A.L., Podlevskih A.P. Ocenka ehffektivnosti vnedreniya v deyatel›nost› organizacii oblachnyh tekhnologij na osnove uproshchennoj metodiki rascheta sovokupnoj stoimosti vladeniya // Fundamental›nye issledovaniya. 2015. № 11(chast› 5). S. 1048-1053.
2 Nikol›skij, Aleksej Valer›evich. Zashchita oblachnyh vychislenij ot atak na sredstva virtualizacii: dissertaciya ... kandidata tekhnicheskih nauk: 05.13.19 / Nikol›skij Aleksej Valer›evich; [Mesto zashchity: S.-Peterb. gos. politekhn. un-t].– Sankt-Peterburg, 2013.– 148 s.
3 Peskova O.YU., Stepovaya K.E. Bezopasnost› kontrolya dostupa k oblachnym sistemam // Informacionnoe protivodejstvie ugrozam terrorizma. 2014. № 23. S.110-120.
4 SHpakov D.V. Izuchenie problemy bezopasnosti oblachnyh tekhnologij // ZHurnal gumanitarnyh nauk. 2017. № 1(17). S.162-166.
5 Peskova O.YU., Stepovaya K.E. Obobshchennye trebovaniya po obespecheniyu bezopasnosti oblachnyh servisov // Informacionnoe protivodejstvie ugrozam terrorizma. 2014. № 23. S.120-130.
6 Zubarev I.V., Radin P.K. Osnovnye ugrozy bezopasnosti informacii v virtual›nyh sredah i oblachnyh platformah // Voprosy kiberbezopasnosti. 2014. № 2(3). S. 40 – 45.
7 Zorin E.L., CHichvarin N.V. Informacionnaya bezopasnost› SAPR/PLM , primenyayushchih oblachnye tekhnologii // Voprosy kiberbezopasnosti. 2014. № 4(7). S. 23 – 29.
8 Glinskaya E.V., CHichvarin N.V. Informacionnaya bezopasnost› otkrytyh kanalov peredachi proektnoj dokumentacii, produciruemoj v SAPR // Voprosy kiberbezopasnosti. 2014. № 4(7) . S. 11 – 22.
9 Borovskij A.S. Integrirovannyj podhod k postroeniyu sistem fizicheskoj zashchity ob»ektov // Nauka i obrazovanie transportu. 2016. №2. S. 12-16.
10 Borovskij A.S. Programmnyj kompleks ocenki inzhenerno-tekhnicheskoj zashchishchennosti potencial›no opasnyh ob»ektov // Programmnye produkty i sistemy. 2014. №3(107). S.141 – 147.
11 Borovskij A.S. Obobshchennaya model› sistemy fizicheskoj zashchity kak ob»ekt avtomatizirovannogo proektirovaniya // Vestnik komp›yuternyh i informacionnyh tekhnologij. 2014. №10. S.45 – 52.
12 Borovskij A.S. Metod opredeleniya optimal›nogo urovnya vozmozhnostej sredstv inzhenerno-tekhnicheskoj zashchity ob»ekta v zadachah proektirovaniya sistem fizicheskoj zashchity // Informacionnye tekhnologii. 2014.№12.S.67 – 75.
13 Kostin V.N., Borovskij A.S. Metod ocenki utechki konfidencial›noj informacii o funkcionirovanii sistemy zashchity ob»ekta informatizacii po informacionnomu kriteriyu // Vestnik komp›yuternyh i informacionnyh tekhnologij. 2016. №8. S.34 – 43.
14 Borovskij A.S., Tarasov A.D. Programmnyj kompleks informacionnoj podderzhki resheniya zadachi proektirovaniya sistemy fizicheskoj zashchity // Sistemy upravleniya i informacionnye tekhnologii. 2016. № 4.1(66). S. 122-128
15 SHidlovskij, V.V. Informacionnaya model› kak osnova sistemy podderzhki prinyatiya reshenij / V.V.SHidlovskij [i dr.] // Informacionnye tekhnologii v proektirovanii i proizvodstve. 2015. № 1 (157). S. 14–21.
16 Melihova, O.A. Obzor modelej sistem prinyatiya reshenij / O.A.Melihova, EH.G.Rudenko, O.A.Loginov // Aktual›nye problemy gumanitarnyh i estestvennyh nauk. 2015. № 6–1. S. 78 – 83.
17 Vyatkin, A.YU. Sistemy podderzhki prinyatiya reshenij – sovremennyj ehtap razvitiya informacionnyh sistem / A.YU.Vyatkin, D.V.Smirnov, I.A.Kochetov // Izvestiya Instituta inzhenernoj fiziki. 2015. T. 1. № 35. S. 40 – 42.
18 Vitenburg E.A. Formalizovannaya model› sistemy intellektual›noj podderzhki prinyatiya reshenij v oblasti zashchity informacii // Izvestiya tul›skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2017. № 7. S. 268 – 274.
19 Lomazov V.A., Gostishcheva T.V., Klimova N.A. Nechetkij analiz ugroz i vybor variantov sistemy informacionnoj bezopasnosti innovacionnogo proekta // Sovremennye naukoemkie tekhnologii. 2017. № 10. S. 26 – 31.
20 Vitenburg E.A., Nikishova A.V., CHurilina A.E. Sistemy podderzhki prinyatiya reshenij v informacionnoj bezopasnosti // Vestnik komp›yuternyh i informacionnyh tekhnologij. 2015. № 4(130). S. 50 – 56.