

УДК 004.056.53

ДЕРЕВЬЯ УЩЕРБОВ КАК МОДЕЛЬ ОЦЕНКИ РИСКОВ ПОТЕРЬ ДОСТУПНОСТИ ПОСЛЕ ПРОВЕДЕНИЯ ИЗМЕНЕНИЙ В ФИНАНСОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

С.А. Арустамов, М.Г. Генин

Рассматривается метод прогнозирования и анализа рисков потерь доступности критических информационных систем с помощью построения деревьев ущербов. Приводится описание метода построения дерева ущербов для каждого из возможных событий, которые могут привести к потере доступности. Приводится пример, иллюстрирующий использование метода, на основании которого можно выбрать наиболее рациональную стратегию тестирования программного обеспечения.

Ключевые слова: информационные системы, оценки, анализ, доступность, риск потери доступности, ущерб, дерево ущербов, стратегия тестирования ПО.

Введение

В работе рассматриваются риски потери доступности программного обеспечения (ПО) при проведении обновлений финансовых информационных систем [1, 2]. Как правило, финансовые информационные системы имеют жесткие требования по доступности. Под доступностью в работе будем понимать возможность системы выполнять заявленные функции их легальными пользователями.

Обычно риск потери доступности [3] определяют как пару, состоящую из вероятности наступления того или иного события, приведшего к потере доступности после проведения обновления, и ущерба от наступления этого события. В настоящей работе предлагается ввести расширенное понятие ущерба в предположении, что он носит вероятностный характер. Например, утрата части клиентской базы и связанная с этим потеря доли рынка в результате сбоя ПО может и не произойти. Все зависит от множества объективных и субъективных факторов, таких как продолжительность неработоспособности системы в результате сбоя, время сбоя, наличие клиентов, которые в момент сбоя работали с системой, и т.д. Исходя из этого, можно говорить как о величине ущерба, так и о вероятности наступления ущерба при условии, что сбой произошел. Основываясь на этих предположениях, определим риск потери доступности следующим образом:

$$R_i = \{P_i, L_i(P_{Li})\}, \quad (1)$$

где R_i – риск наступления i -го события; P_i – вероятность наступления i -го события; $L_i(P_{Li})$ – величина ущерба от i -го события, наступающая с вероятностью P_{Li} , при этом ущерб будем рассматривать как дискретную случайную величину (ДСВ).

Будем считать, что на момент начала исследования текущая версия системы до обновления не содержит ошибок, т.е. риски потери доступности для нее отсутствуют. Предметом исследования является обнаружение и предотвращение в максимально короткие сроки проблем, которые могут возникнуть в результате обновления системы. Для решения данной задачи предлагается следующий подход. Для каждого из выявленных возможных негативных событий (сбоев), которые могут иметь место в результате обновления¹, проводится оценка риска потери доступности на основе анализа возможных ущербов от этого события. События с более высоким риском признаются более опасными. На основе этого строится стратегия тестирования обновления, по которой приоритет отдается тестированию компонентов ПО с высокими рисками. Для количественной оценки риска потери доступности в работе предлагается метод построения дерева ущерба для каждого из выявленных негативных событий. Вопросы технологии тестирования ПО не являются предметом данной работы.

Построение дерева ущербов для i -го события

Продолжим дальше развивать понятие ущерба. Обратим внимание на то, что ущерб L_i , возникший в результате события i , может быть, вообще говоря, составным, т.е. может быть разложен на несколько независимых составляющих:

$$L_i = \{L_{ij}\}, j = \{1, 2, \dots, N\},$$

¹ Выявление проведенных обновлений автоматически отслеживается программными агентами, установленными на критических узлах системы. Сведения о проведенных изменениях передаются на централизованный сервер.

где L_{ij} – j -я составляющая ущерба L_i , возникшего в результате i -го события. В самом деле, в результате сбоя системы могут иметь место одновременно и независимо друг от друга несколько негативных последствий. Например, в результате неполадок новой версии СУБД перестали быть доступными независимые друг от друга функции (такие, например, как ввод документов и подготовка отчетности). Как следствие, возникает несколько независимых друг от друга ущербов. Продолжая цепочку рассуждений дальше, по аналогии с (1), можно заметить, что у каждой j -й составляющей ущерба L_{ij} может быть своя вероятность возникновения $P_{L_{ij}}$, которая не зависит от других составляющих. Отталкиваясь от приведенного выше примера, можно предположить, что ущерб в результате невозможности ввода документов никак не связан с ущербом из-за проблем модуля подготовки отчетности. Вероятность возникновения первого связана с возможным недовольством клиентов или руководителей, а вторая – с возможными штрафными санкциями со стороны надзорных органов. В результате получаем следующее выражение для риска потери доступности:

$$R_i = \{P_i, \{L_{i1}(P_{L_{i1}}), L_{i2}(P_{L_{i2}}), L_{i3}(P_{L_{i3}}), \dots, L_{iN}(P_{L_{iN}})\}\}, \quad (2)$$

где N – количество независимых составляющих ущерба от i -го события.

Рассмотрим теперь ситуацию, когда составляющие ущерба являются зависимыми друг от друга, т.е. когда одна составляющая ущерба является следствием другой. Это возможно в случае, когда в результате неполадок в работе системы часть клиентов переходит к другому поставщику услуг, в результате чего уменьшается доля контролируемого рынка, и т.д. Возникает ситуация, когда один ущерб может вызвать другой, и т.д., т.е. возникает цепочка вложенных ущербов. Каждый из ущербов в цепочке имеет свою собственную вероятность возникновения, но при условии, что реализовались все предыдущие ущербы из цепочки. В данном примере уменьшение доли рынка возможно только при переходе части клиентов к другому поставщику, а переход на другую платформу возможен, в свою очередь, только как следствие неполадок в работе системы. В этом случае риск потери доступности для зависимых случайных величин можно определить следующим образом:

$$R_i = \{P_i, \{L_{i1}(P_{L_{i1}}), L_{i2}(P_{L_{i2}/L_{i1}}), \dots, L_{iN}(P_{L_{iN}/L_{iN-1} \dots L_{i3}L_{i2}L_{i1}})\}\}, \quad (3)$$

где N – количество зависимых ущербов от i -го события в данной цепочке.

Возможно существование ситуаций, когда цепочка зависимых ущербов завершается несколькими независимыми друг от друга ущербами, каждый из которых, в свою очередь, может быть началом новой цепочки зависимых ущербов, т.е. присутствует комбинация зависимых и независимых ДСВ.

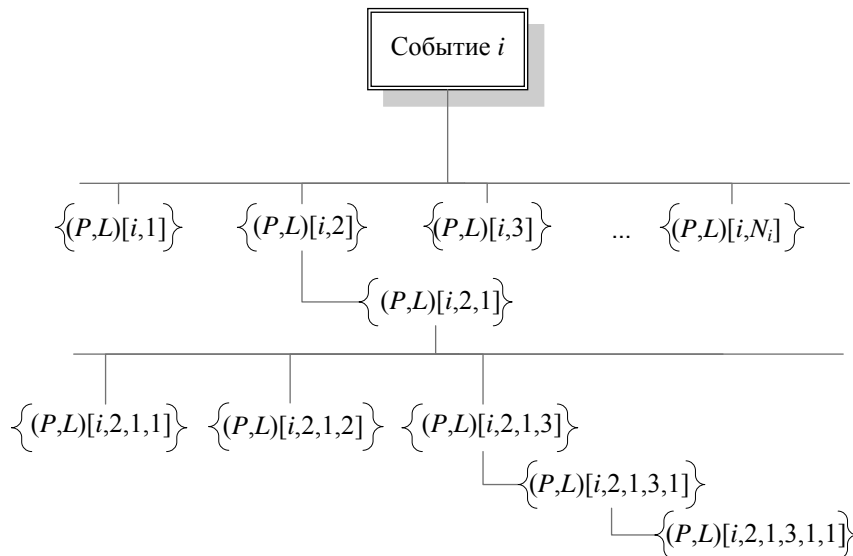


Рис. 1. Графическое изображение дерева ущербов, порождаемого i -м событием

В общем случае можно сказать, что в результате события i может иметь место набор независимых ущербов, некоторые из которых могут, в свою очередь, породить цепочку зависимых. Каждая из порожденных цепочек зависимых ущербов может, в свою очередь, заканчиваться несколькими независимыми ущербами, которые тоже могут порождать свои цепочки, и т.д. Формально это можно описать различными вложенными комбинациями формул (2) и (3), однако представить общий случай в виде одной формулы сложно, так как выражение будет слишком громоздким. Вместо этого предлагается вариант графического представления совокупности ущербов в виде дерева.

Перед тем, как начать построение дерева, перейдем к более удобному, на наш взгляд, способу обозначения пары «вероятность–ущерб». Вместо нижних индексов будем использовать индексы, заключенные в квадратные скобки. Такие обозначения используются, например, для описания многомерных массивов. Индексы в скобках будем указывать сразу для пары (P, L) , а не для каждой из составляющих, так

как индексы для P и для L из одной пары всегда совпадают. Например, запись $L_{i1}(P_{i1})$ преобразуется в $(P, L)[i, 1]$. Тогда запись (3) для независимых ущербов будет выглядеть следующим образом:

$$R_i = \{P_i, \{(P, L)[i, 1], (P, L)[i, 2], (P, L)[i, 3], \dots, (P, L)[i, N_i]\}\},$$

где N_i – количество независимых составляющих ущерба от i -го события.

Для обозначения ущерба, подчиненного предыдущему, мы будем использовать индекс следующего уровня. Например, ущерб, который подчинен ущербу $(P, L)[i, 2]$, мы будем обозначать как $(P, L)[i, 2, 1]$, следующий за ним в цепочке ущерб будет уже $(P, L)[i, 2, 1, 1]$, и т.д. Запись (3) для зависимых ущербов в новой форме будет такой:

$$R_i = \{P_i, \{(P, L)[i, 1], (P, L)[i, 1, 1], (P, L)[i, 1, 1, 1], \dots, (P, L)[i, 1, \dots, 1]\}\}.$$

Например, если у узла $(P, L)[i, 1, 1]$ будет не один подчиненный ему ущерб, а N_i подчиненных ущербов, независимых друг от друга, то будем обозначать их как $(P, L)[i, 1, 1, 1]$, $(P, L)[i, 1, 1, 2]$, $(P, L)[i, 1, 1, 3]$, ..., $(P, L)[i, 1, 1, N_i]$.

Используя данный подход к обозначению ущербов разных уровней (узлов дерева), мы можем для наглядности перейти к модели ущербов в виде дерева (рис. 1).

Свертка дерева ущерба для i -го события. Ожидаемое значение ущерба

Выше было рассмотрено разложение ущерба из формулы (1) на составляющие с помощью построения дерева ущербов. Тем не менее, общий возможный ущерб, указанный в формуле (1), наряду с его составными частями, также имеет смысл как отдельная числовая величина, а разложение его на составляющие в виде дерева ущерба – это лишь вариант представления общего ущерба. Следовательно, должен существовать способ преобразования данных из дерева ущербов в величину общего возможного ущерба из формулы (1). Назовем эту величину ожидаемым значением ущерба L_i^{est} .

Для ее вычисления будем применять подход, основанный на расчете математического ожидания случайной величины. Вначале отдельно рассмотрим варианты расчета математического ожидания для независимых и зависимых ущербов, а затем их комбинацию для расчета ожидаемого значения ущерба для всего дерева.

Для независимых событий (горизонтальный уровень дерева) средневзвешенное значение ДСВ (математическое ожидание) вычисляется как сумма произведений вероятности и величины каждой из возможных комбинаций ущербов, разделенная на сумму вероятностей комбинаций этих ущербов. Так как перечисляются все возможные комбинации независимых ущербов одного горизонтального уровня, то их совокупность можно считать полной группой событий, поэтому сумма вероятностей всех возможных комбинаций, т.е. знаменатель формулы, будет равен единице.

Рассмотрим дерево k при гипотезе, что число его независимых ущербов горизонтального уровня равно 2. Для простоты записи обозначим вероятность j -ого ущерба P_j^k , а его величину L_j^k ($j = 1, 2$). Тогда ожидаемое значение ущерба для дерева k будет следующим:

$$L_k^{est} = \frac{P_1^k \cdot (1 - P_2^k) \cdot L_1^k + P_2^k \cdot (1 - P_1^k) \cdot L_2^k + P_1^k \cdot P_2^k \cdot (L_1^k + L_2^k) + (1 - P_1^k) \cdot (1 - P_2^k) \cdot L^k(0)}{P_1^k \cdot (1 - P_2^k) + P_2^k \cdot (1 - P_1^k) + P_1^k \cdot P_2^k + (1 - P_1^k) \cdot (1 - P_2^k)}, \quad (4)$$

где $L^k(0) = 0$ – нулевая величина ущерба, соответствующая исходу, при котором он отсутствует.

Так как $L^k(0) = 0$, а знаменатель, образуя сумму вероятностей полной группы событий (ущербов), равен единице, то формула (4) примет следующий вид:

$$L_k^{est} = P_1^k \cdot (1 - P_2^k) \cdot L_1^k + P_2^k \cdot (1 - P_1^k) \cdot L_2^k + P_1^k \cdot P_2^k \cdot (L_1^k + L_2^k). \quad (5)$$

После аналогичных рассуждений и преобразований для дерева m с гипотезой о трех независимых ущербах формула расчета ожидаемого ущерба примет вид

$$\begin{aligned} L_m^{est} = & P_1^m \cdot (1 - P_2^m) \cdot (1 - P_3^m) \cdot L_1^m + P_2^m \cdot (1 - P_1^m) \cdot (1 - P_3^m) \cdot L_2^m + P_3^m \cdot (1 - P_1^m) \cdot (1 - P_2^m) \cdot L_3^m + \\ & + P_1^m \cdot P_2^m \cdot (1 - P_3^m) \cdot (L_1^m + L_2^m) + P_2^m \cdot P_3^m \cdot (1 - P_1^m) \cdot (L_2^m + L_3^m) + P_1^m \cdot P_3^m \cdot (1 - P_2^m) \cdot (L_1^m + L_3^m) + \\ & + P_1^m \cdot P_2^m \cdot P_3^m \cdot (L_1^m + L_2^m + L_3^m). \end{aligned} \quad (6)$$

В общем случае с $N > 3$ независимыми составляющими ущерба от i -го события формула для вычисления L_i^{est} будет очень громоздкой, поэтому в работе она не приведена. Кроме того, на практике крайне редко удается выделить более трех независимых существенных ущербов, порождаемых одним узлом дерева.

При суммировании зависимых ущербов одной ветви дерева будем использовать тот же подход, что и для (5)–(6), перебирая все возможные комбинации ущербов для ветви дерева, но учитывая при этом, что реализация каждого следующего ущерба из данной ветви возможна при условии, что все предыдущие ущербы реализовались. В отличие от независимых ущербов одного горизонтального уровня, совокупность зависимых ущербов вертикальной ветви не образует полную группу событий, так как не все возможные комбинации реализуются. Ущерб d не может реализоваться в случае, если не реализовались ущербы $1, 2, \dots, (d-1)$.

Рассмотрим дерево q при гипотезе, что оно состоит из одной ветви, содержащей три последовательных ущерба ($d = 3$). В этом случае ожидаемое значение ущерба примет вид

$$L_q^{est} = \frac{(1 - P_1^q) \cdot L^q(0) + P_1^q \cdot (1 - P_2^q) \cdot (1 - P_3^q) \cdot L_1^q + P_1^q \cdot P_2^q \cdot (1 - P_3^q) \cdot (L_1^q + L_2^q) + P_1^q \cdot P_2^q \cdot P_3^q \cdot (L_1^q + L_2^q + L_3^q)}{(1 - P_1^q) + P_1^q \cdot (1 - P_2^q) \cdot (1 - P_3^q) + P_1^q \cdot P_2^q \cdot (1 - P_3^q) + P_1^q \cdot P_2^q \cdot P_3^q}, \quad (7)$$

где $L^q(0)$ – нулевой ущерб. Так как $L^q(0) = 0$, то формула (7) примет следующий вид:

$$L_q^{est} = \frac{P_1^q \cdot (1 - P_2^q) \cdot (1 - P_3^q) \cdot L_1^q + P_1^q \cdot P_2^q \cdot (1 - P_3^q) \cdot (L_1^q + L_2^q) + P_1^q \cdot P_2^q \cdot P_3^q \cdot (L_1^q + L_2^q + L_3^q)}{(1 - P_1^q) + P_1^q \cdot (1 - P_2^q) \cdot (1 - P_3^q) + P_1^q \cdot P_2^q \cdot (1 - P_3^q) + P_1^q \cdot P_2^q \cdot P_3^q}. \quad (8)$$

Поскольку совокупность зависимых ущербов вертикальной ветви не образует полную группу событий, знаменатель формулы (7) будет всегда меньше единицы, поэтому его придется учитывать при расчете ожидаемого значения ущерба для зависимых событий ветви дерева.

С использованием этой методики можно рассчитать ожидаемое значение ущерба для всего дерева. Вначале, используя (8), будем проводить свертку от концов самых нижних ветвей до нижних горизонтальных уровней. Затем, в соответствии с (5)–(6), будем проводить свертку самих этих горизонтальных уровней. Повторяя эти две операции, мы постепенно свернем все дерево, двигаясь снизу вверх от самых длинных ветвей к вершине. На рис. 2 показан пример процесса поэтапной свертки дерева ущербов.

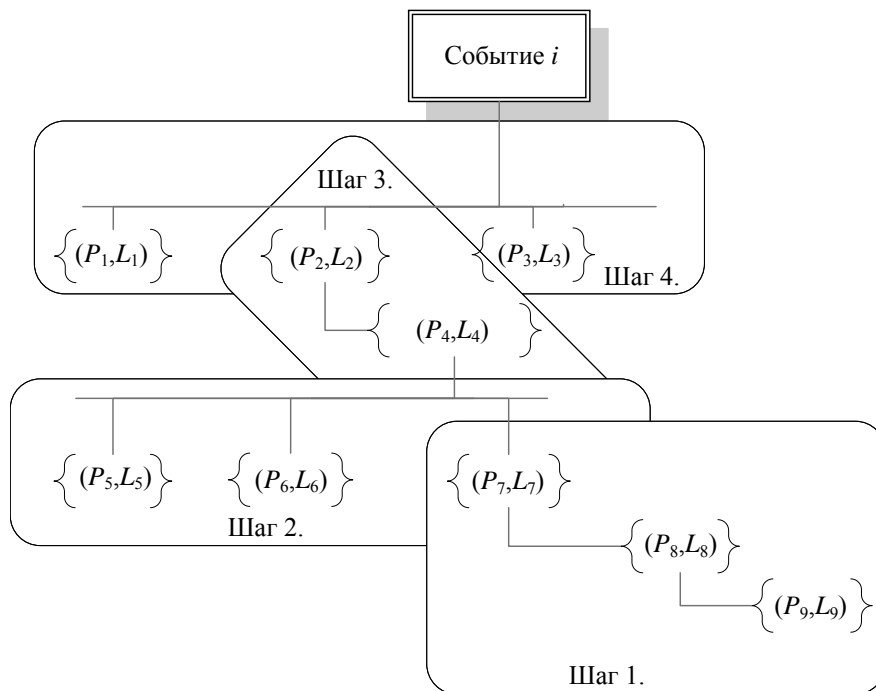


Рис. 2. Пример пошагового алгоритма свертки для дерева ущербов

Ниже приведена последовательность действий по расчету ожидаемого значения ущерба для данного дерева в соответствии с шагами, показанными на рис. 2.

Шаг 1.

$$L^{est1} = L_7 + \frac{P_8 \cdot (1 - P_9) \cdot L_8 + P_8 \cdot P_9 \cdot (L_8 + L_9)}{(1 - P_8) + P_8 \cdot (1 - P_9) + P_8 \cdot P_9}.$$

Так как узел $\{(P_7, L_7)\}$ является не только источником зависимых ущербов $\{(P_8, L_8)\}$ и $\{(P_9, L_9)\}$, но также принадлежит горизонтальному уровню с независимыми ущербами $\{(P_5, L_5)\}$ и $\{(P_6, L_6)\}$, его вероятность P_7 будет учтена на следующем шаге. Аналогичным образом будем действовать ниже для узлов $\{(P_4, L_4)\}$ и $\{(P_2, L_2)\}$.

Шаг 2.

$$L^{est2} = L_4 + P_5 \cdot (1 - P_6) \cdot (1 - P_7) \cdot L_5 + (1 - P_5) \cdot (1 - P_7) \cdot P_6 \cdot L_6 + (1 - P_5) \cdot (1 - P_6) \cdot P_7 \cdot L^{est1} + P_5 \cdot P_6 \cdot (1 - P_7) \cdot (L_5 + L_6) + P_5 \cdot P_7 \cdot (1 - P_6) \cdot (L_5 + L^{est1}) + P_6 \cdot P_7 \cdot (1 - P_5) \cdot (L_6 + L^{est1}) + P_7 \cdot P_8 \cdot P_9 \cdot (L_5 + L_6 + L^{est1}).$$

Шаг 3.

$$L^{est3} = L_2 + \frac{P_4 \cdot L^{est2}}{(1 - P_4) + P_4}.$$

Шаг 4.

$$L^{est} = P_1 \cdot (1 - P_2) \cdot (1 - P_3) \cdot L_1 + (1 - P_1) \cdot P_2 \cdot (1 - P_3) \cdot L^{est3} + (1 - P_1) \cdot (1 - P_2) \cdot P_3 \cdot L + \\ + P_1 \cdot P_2 \cdot (1 - P_3) \cdot (L_1 + L^{est3}) + P_1 \cdot P_3 \cdot (1 - P_2) \cdot (L_1 + L_3) + P_2 \cdot P_3 \cdot (1 - P_1) \cdot (L^{est3} + L_3) + \\ + P_1 \cdot P_2 \cdot P_3 \cdot (L_1 + L^{est3} + L_3).$$

Использование ожидаемого значения ущерба для того или иного события после свертки всего дерева ущербов позволяет получить некоторую обобщенную оценку величины возможного ущерба от данного события. Эту оценку можно будет использовать в дальнейшем при анализе риска потери доступности при возникновении данного события. Кроме того, для любого события r , связанного с потерей доступности ПО, наряду с ожидаемым значением ущерба L_r^{est} логично ввести понятие максимального значения ущерба L_r^{max} , которое рассчитывается при условии, что вероятность любого из составляющих ущербов события r равна единице.

Градации ущербов и вероятностей

Для выполнения операций сложения и сравнения величин дискретных вероятностных ущербов необходимо, чтобы их величины были одной размерности. В то же время природа ущерба может быть самой разной (финансовой, имиджевой, временной и т.д.), поэтому свести имиджевые, временные потери или санкции надзорных органов (отбор лицензии, запрет на выполнение определенных видов деятельности и т.д.) к некоторой заранее рассчитанной денежной величине может быть крайне затруднительно. При невозможности расчета абсолютных величин ущербов в денежном выражении предлагается перейти от абсолютных значений величин ущерба к некоторым условным значениям, тем самым упростив данную модель.

Представим ущерб в некоторых условных единицах, соответствующих степени его существенности для нас, например, очень низкий, низкий, средний, высокий и очень высокий. Для того чтобы с величинами ущербов можно было выполнять операции сложения и умножения, поставим в соответствие величинам ущербов числовой ряд {1, 2, 3, 4, 5} так, что числу 5 соответствует максимальный ущерб (табл. 1).

Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
1	2	3	4	5

Таблица 1. Градации величин ущербов

Перейдем ко второй компоненте ущерба – вероятности. Поступим так же, как поступали при оценке величины ущерба: введем градации вероятности. Будем использовать три уровня вероятности ущерба: низкую (Н), среднюю (С), высокую (В), поставив им в соответствие числовой ряд {0,3; 0,6; 0,9}² (табл. 2).

Низкий (Н)	Средний (С)	Высокий (В)
0,3	0,6	0,9

Таблица 2. Градации вероятностей ущербов

После введения градаций величин ущербов и их вероятностей можно перейти к оценке ущерба в целом как пары «вероятность–величина», используя механизм расчета расчетного значения ущерба, описанный в предыдущем разделе.

Ущерб и продолжительность потери доступности

При построении дерева ущербов представляется целесообразным учитывать возможное изменение вероятности возникновения или величины того или иного ущерба от продолжительности потери доступности системы. Приведем некоторые примеры в подтверждение этого.

1. Вероятность вынесения штрафных санкций за задержку при сдаче отчетности равна единице вне зависимости от времени задержки. Величина штрафа зависит от длительности задержки: к основной сумме добавляются пени. В данном случае от времени зависит только величина ущерба.
2. Вероятность перехода того или иного клиента на другую систему зависит от времени неработоспособности. Величина ущерба при уходе одного клиента не зависит от времени и является фиксированной величиной.

² Предложенное авторами разбиение представляется удобным с точки зрения программной реализации. Можно использовать и другую шкалу градаций величин ущербов и вероятностей, которую можно настраивать в зависимости от сложности эксплуатируемой инфраструктуры.

Перейдем теперь к описанию этих ситуаций в модели дерева ущербов. С точки зрения вероятности целесообразно рассмотреть две ситуации:

1. сохранение во времени вероятности, указанной на момент, когда ущерб может возникнуть (В–В–...–В);
2. рост вероятности ущерба при простое системы (Н–...–Н–С–...–С–В–...–В).

С точки зрения оценки эволюции величины ущерба во времени ситуация аналогична: величина ущерба либо такая же, как была указана на начальный момент времени существования данного ущерба, либо возрастает по мере простоя системы³.

Для некоторых типов ущербов, таких как пени за просрочку штрафа, зависимость вероятности и величины ущерба от времени можно точно указать, зная величину штрафа и пени за просрочку. Для оценки других видов ущербов придется выдвигать предположения на основе экспертных оценок.

Таким образом, анализируя возможный рост вероятности и величины ущерба для каждого из ущербов в построенном дереве, можно перейти от статического изображения дерева ущербов к его динамическому изображению, указав возможную эволюцию во времени каждого из ущербов дерева. Стоит отметить, что как ожидаемое значение ущерба L_i^{est} , так и максимальный ущерб L_i^{max} тоже будут зависеть от продолжительности простоя системы.

Описание тестов предложенной методики

Для исследования эффективности предложенной методики использовалась тестовая ИТ-инфраструктура финансового-кредитного учреждения, на которой была установлена обновленная система дистанционного банковского обслуживания и проведены изменения инфраструктуры, необходимые для ее функционирования. Предметом исследования были выявление и предотвращение в максимально короткие сроки возможных проблем, которые могли возникнуть в результате изменений компонентов финансовой информационной системы.

Обновление затрагивало следующие компоненты системы: административный модуль (АМ), модуль рублевых платежей (РП), а также модуль обмена с внешними подсистемами (ОВП).

На основе анализа возможных проблем при обновлении каждого из указанных компонентов был получен список возможных негативных событий (уязвимостей), связанный с обновлениями этих компонентов (табл. 3).

Модуль	Уязвимость
АМ	Некорректная обработка прав существующих пользователей
АМ	Ошибки при заведении новых пользователей/изменении прав существующих пользователей
РП	Ошибки при заведении клиентом платежей нового формата ускоренной доставки
РП	Ошибки при заведении клиентом платежей старых форматов
ОВП	Ошибки при обработке платежей нового формата ускоренной доставки на стороне банка
ОВП	Ошибки при обработке платежей старых форматов на стороне банка

Таблица 3. Список возможных уязвимостей

При построении дерева ущербов для каждого из выявленных событий использовались условные, а не абсолютные значения ущербов. В результате анализа деревьев ущербов, построенных для случая возможной неработоспособности каждого из перечисленных компонентов, были получены значения ожидаемых L_i^{est} и максимальных L_i^{max} ущербов (табл. 4).

На основе полученных данных были сделаны следующие выводы. Значения обоих параметров L_i^{est} и L_i^{max} однозначно указывают на события с максимальными возможными ущербами, на предотвращение которых надо обратить особое внимание при тестировании: (1), (6), (4) (см. табл. 4). Вместе с тем, для событий с меньшими возможными ущербами параметр L_i (свертка всех ущербов для дерева данного события) дает более точную оценку и позволяет различать события с одинаковыми параметрами L_i^{max} – простая сумма всех ущербов для дерева (2), (3) (см. табл. 4). Несмотря на то, что эти различия незначительны, тестировать систему с целью предотвращения обоих событий нужно практически с одним и тем же приоритетом.

В целом на основании проведенного анализа можно сделать вывод о том, что в данном случае расчета параметра L_i^{max} (простой суммы ущербов по каждому из событий) вполне достаточно для проведения сравнительной оценки рискованности выявленных событий и выбора стратегии тестирования. Тем не менее, в связи с многообразием ситуаций, связанных с расчетом ущербов, порождаемых негативными

³ Ситуации, при которых вероятность или величина ущерба снижаются по мере простоя системы, авторами не рассматриваются, так как не имеют практического смысла.

событиями, целесообразно анализировать как общую сумму ущербов L_i^{\max} , так и свертку величин ущербов по вероятности L_i^{est} , так как учет вероятностей ущербов дает дополнительную информацию для выбора стратегии тестирования.

Модуль	Уязвимость	Возможное время неработоспособности					
		1 час		4 часа		8 часов	
		L_i^{est}	L_i^{\max}	L_i^{est}	L_i^{\max}	L_i^{est}	L_i^{\max}
АМ	Некорректная обработка прав существующих пользователей (1)	3,51	6	8,79	12	18,49	29
АМ	Ошибки при заведении новых пользователей/ изменении прав существующих пользователей (2)	0,3	1	0,78	2	7,53	10
РП	Ошибки при заведении клиентом платежей нового формата ускоренной доставки (3)	0,3	1	0,63	2	6,26	10
РП	Ошибки при заведении клиентом платежей старых форматов (4)	3,32	6	8,78	12	12,2	15
ОВП	Ошибки при обработке платежей нового формата ускоренной доставки на стороне банка (5)	0,3	1	0,78	2	3,51	6
ОВП	Ошибки при обработке платежей старых форматов на стороне банка (6)	6,41	12	10,98	15	18,43	25

Таблица 4. Оценка ожидаемых и максимальных ущербов для выявленных уязвимостей

Заключение

В работе был рассмотрен метод прогнозирования риска потери доступности финансовых информационных систем на основе построения деревьев ущербов для выявленных возможных негативных событий. На основе полученных данных созданы предпосылки для выбора рациональной стратегии тестирования программного обеспечения за счет детального учета информации, необходимой для принятия обоснованных решений. Проведены эксперименты, результаты которых подтверждают эффективность предложенной методики.

Литература

1. Арустамов С.А., Генин М.Г. Минимизация рисков потери доступности программного обеспечения после установки обновлений или изменения функциональности // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 3 (73). – С. 111–116.
2. Генин М.Г. Методика проведения обновлений, снижающая риски доступности информационных ресурсов. Информатика, моделирование, автоматизация проектирования // Сборник научных трудов под ред. Н.Н. Войта. – Ульяновск: УлГТУ, 2011. – С. 125–137.
3. Арустамов С.А., Генин М.Г. Методы снижения рисков потерь доступности программного обеспечения критических информационных систем // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 131–136.

Арустамов Сергей Аркадьевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, профессор, sergey.arustamov@gmail.com

Генин Михаил Геннадьевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, gmg@rambler.ru