В. С. Аткина

ПРИМЕНЕНИЕ КАРТЫ РИСКОВ ДЛЯ ОЦЕНКИ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ СУЩЕСТВЕННОЙ СРЕДЫ НА ИНФОРМАЦИОННУЮ СИСТЕМУ

Введение

В настоящее время одной из актуальных проблем в области обеспечения защиты информационных технологий и управления информационной безопасностью любой организации в целом, вне зависимости от принадлежности ее к государственному или частному сектору экономики, является проблема обеспечения непрерывности бизнеса и доступности информационных систем, осуществляющих обработку данных и выполнение ключевых бизнес-процессов. И это не только обуславливается современной действительностью, когда от времени доступа к информации или обработки какого-либо запроса зависит конкурентоспособность организации на рынке, но и регламентируется рядом внешних требований к непрерывности, описанных в российском федеральном законодательстве, постановлениях правительства, стандартах и нормативно-методических документах [1–6]. К наиболее значимым из данных требований можно отнести:

— требования к обеспечению бесперебойности осуществления перевода электронных денежных средств операторами электронных денежных средств;

— требования к составлению плана действий и мероприятий в случае наступления катастрофы, а также перечень и периодичность проведения регламентных работ по обеспечению отказоустойчивости;

— требования к кредитным организациям различного уровня по разработке и ведению процедур резервирования (копирования) данных и процедур восстановления функций автоматизированных информационных систем;

— обязанность государственных органов и органов местного самоуправления обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления [3. С. 10];

— требования к операторам федеральных государственных информационных систем обеспечить восстановление информации, измененной или уничтоженной вследствие несанкционированного доступа к ней, в течение не более 8 часов;

— требования по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования;

— требования, предъявляемые к системам персональных данных, по незамедлительному восстановлению персональных данных.

Таким образом, можно сделать вывод о том, что при обеспечении непрерывности бизнеса и восстановления деятельности в части информационных систем обязательные требования надо учитывать:

— банкам;

— государственным органам и органам местного самоуправления;

— ключевой системе информационной инфраструктуры (КСИИ);

— операторам персональных данных.

Следовательно, актуальными задачами в этом случае являются изучение и совершенствование подходов к исследованию, анализу и синтезу информационных систем с высокими показателями

катастрофоустойчивости и надежности функционирования в условиях деструктивного воздействия различного рода катастроф и дестабилизирующих факторов (ДФ). Таким образом, в рамках данной работы автором под дестабилизирующим фактором будет пониматься угроза, реализация которой приводит к исчезновению устойчивого состояния информационной системы, нарушению непрерывности функционирования и переходу системы из «благоприятного» (с точки зрения реализации целей) в небезопасное состояние.

1. Анализ дестабилизирующих факторов

В условиях больших городов существует большое число чрезвычайных ситуаций и катастроф, происходящих в любом районе города, — от элементарного пожара до террористического акта или блокировки здания правоохранительными органами. Все эти потенциально возможные катастрофы и дестабилизирующие факторы являются трудно прогнозируемыми и могут быть различной природы и характера [7]:

— природные катастрофы и стихийные бедствия: землетрясение, наводнение, оползень, подмыв грунтовыми водами, сильнейшие морозы и т. п.;

— технологические катастрофы: просадка здания, обрыв кабеля из-за строительных работ, сбой в серверной из-за прорвавшейся водопроводной трубы или отключившегося в непредвиденно жаркую погоду кондиционера и т. д.;

— юридические дестабилизирующие факторы: неправильно оформленный договор аренды с последующим вынужденным выселением и т. д.;

— социальные катастрофы: терроризм, беспорядки в районе, эпидемия и т. д.

В соответствии с подходом, предложенным автором в работе [7], считаем, что все возможные катастрофы и дестабилизирующие факторы будут порождаться внешней по отношению к информационной системе (ИС) организации существенной средой, с которой ИС постоянно взаимодействует в процессе своего функционирования и реализации бизнес-процессов организации-владельца.

Данные дестабилизирующие факторы могут оказать деструктивное воздействие как на саму ИС организации или ее отдельные компоненты, так и на обеспечивающую инфраструктуру макрообъекта, внутри которого располагается ИС, в результате чего может возникнуть недоступность:

— здания;
— персонала;
— ИТ и телекоммуникаций;
— информации;
— прочих технологий;
— резерва ликвидных средств (для финансовых организаций);
— внешних ключевых провайдеров, без которых немыслима деятельность организации.

Как следствие, работа всей организации или ее существенной части прерывается. На ликвидацию последствий деструктивных воздействий и восстановление деятельности, по данным исследований компаний Symanic и DRII, обычно уходит от нескольких минут до нескольких месяцев. Именно в этот период существует серьезная вероятность не выполнить минимальный объем обязательств (перед клиентами, регуляторами, иными заинтересованными сторонами) и в итоге потерять ключевые позиции на рынке, ключевых клиентов, лицензию на деятельность, понести потери, после которых просто невозможно восстановить деятельность, и т. д. То есть в этот период существует риск потери всего бизнеса или его существенной части. По статистике DRII, 93 % компаний, не имевших системы непрерывности бизнеса, не продержались и 5 лет на рынке после деструктивного воздействия катастроф, а 50 % компаний, которые восстанавливали свою деятельность более 10 дней, так и не смогли восстановить ее.

2. Подход к оценке рисков в катастрофоустойчивой информационной системе

Поскольку не все множество ДФ существенной среды способно частично или полностью уничтожить ИС и инфраструктуру организации, то при разработке катастрофоустойчивых решений необходимо в первую очередь оценить опасность всех потенциально возможных ДФ существенной среды и выбрать только те из них, которые могут оказать непосредственное влияние на информационные системы и опорную инфраструктуру. Графически это может быть представлено в виде карты рисков.

Для наиболее существенных рисков, с которыми организация может столкнуться (пожар, отключение электроснабжения, взрыв и т. д.), разрабатываются подробные планы действий, направленные на минимизацию последствий от происшествия, и внедряются соответствующие катастрофоустойчивые решения.

Для оценки рисков автором предлагается использовать количественно-качественный подход, основанный на составлении карты рисков. Согласно данной карте все риски разделяются на три основные зоны:

— зона I — риски, которые компания готова принять, — допустимые;

— зона II — риски, которые нужно контролировать и принимать меры по их снижению;

— зона III — риски, требующие превентивных мер по их предотвращению или снижению их влияния.

Поскольку риск — это мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы [6], то при оценке рисков, связанных с возможным воздействием ДФ существенной среды на ИС организации, необходимо для каждого ДФ определить значения таких характеристик, как вероятность реализации и ущерб. Следовательно, каждый ДФ существенной среды $DF_i \in DF, i = 1..n$, где n — количество ДФ, можно представить следующим вектором значений $DF_i = (\rho, u, risk)$, где ρ — вероятность реализации ДФ, u — потенциально возможный ущерб. Для расчета количественных значений риска используется формула (1):

$$risk = u * \rho. \quad (1)$$

Оценка вероятности реализации ДФ производится либо экспертным путем, либо на основании накопленных статистических данных, характерных для данного региона и условий эксплуатации, и может быть выражена как в количественной, так и в качественной форме. Таким образом, вероятность реализации ДФ существенной среды ρ_i, с областью определения $\rho = [0,1]$, может быть задана следующим множеством базовых значений T_ρ = {нереализуемая, минимальная, средняя, высокая, критичная} = $\{\alpha_{x1}, \alpha_{x2}, \alpha_{x3}, \alpha_{x4}, \alpha_{x5}\}$. В таблице представлена шкала соответствия между количественной и качественной формами оценки вероятности реализации ДФ.

Таблица 1. Шкала соответствия величины, характеризующей вероятность реализации ДФ, выраженной в качественной и количественной формах

Степень реализации ДФ (T_ρ)	Вероятность реализации ДФ ($\rho_{кол}$)
нереализуемая	0
минимальная	(0; 0,2]
средняя	(0,2; 0,5]
высокая	(0,5; 1)
критичная	1

Оценка потенциально возможного ущерба от реализации ДФ существенной среды тесно связана с величиной капитала организации — владельца ИС и также формируется экспертным путем. Величина ущерба от реализации ДФ u_i задается множеством базовых значений T_U = {минимальная, средняя, высокая, критичная} = $\{\alpha_{y1}, \alpha_{y2}, \alpha_{y3}, \alpha_{y4}\}$. Шкала соответствия между количественными и качественными значениями представлена в таблице 2.

Таблица 2. Шкала соответствия величины потенциально возможного ущерба от реализации ДФ, выраженного в качественной и количественной формах

Величина ущерба (T_U)	Величина ущерба ($U_{кол}$)
минимальная	до 1 % от величины капитала организации
средняя	от 1 до 5 % от величины капитала организации
высокая	от 5 до 10 % от величины капитала организации
критичная	более 10 % от величины капитала организации

3. Формирование трехзонной карты рисков

Для сопоставления оценок вероятности реализации ДФ и величины потенциально возможного ущерба формируется карта рисков, которую можно описать множеством $RiskMap = RiskZ1 \cup RiskZ2 \cup RiskZ3$, где RiskZ1, RiskZ2, RiskZ3 — множества, описывающие три зоны риска соответственно. При этом верно, что риск для каждого ДФ существенной среды относится к одной из трех выделенных зон карты рисков: $(risk_i \in RiskZk \mid \forall k = 1..3, RiskZk \subset RiskMap)$. Составление карты рисков осуществляется в соответствии с правилом, составленным в соответствии с системой нечетких высказываний $\tilde{L}^1$, описанной формулой, представленной ниже, и рис. 1.

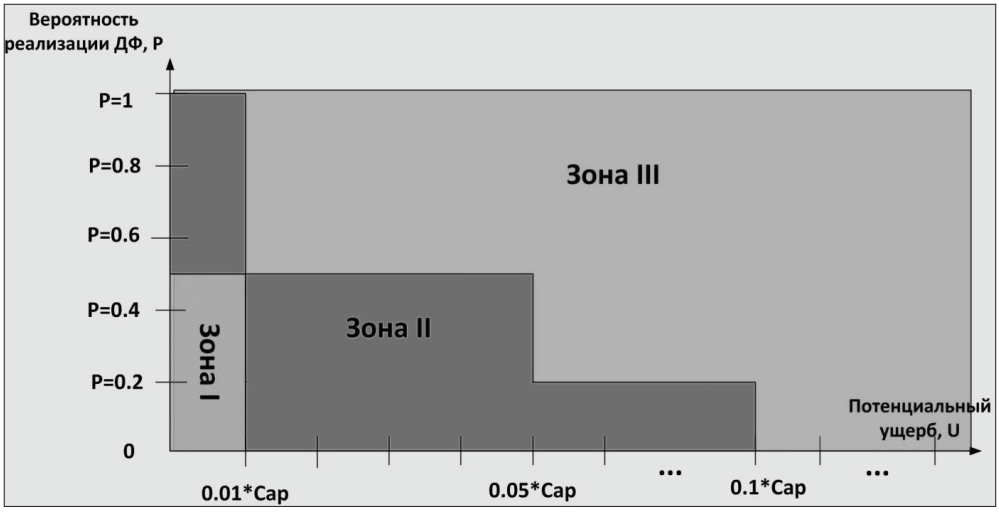

Рис. 1. Карта риска для оценки дестабилизирующих факторов существенной среды

$$\tilde{L}^1 = \begin{cases} \tilde{L}_1^{(1)} :< ЕСЛИ\ E_{11}\ ИЛИ\ E_{12}\ ИЛИ\ E_{13}\ ИЛИ\ E_{14}\ ИЛИ\ E_{21}\ ИЛИ\ E_{31}\ \text{ТО}\ risk_i\ есть\ RiskZ1 >; \\ \tilde{L}_2^{(1)} :< ЕСЛИ\ E_{22}\ ИЛИ\ E_{23}\ ИЛИ\ E_{32}\ ИЛИ\ E_{41}\ \text{ТО}\ risk_i\ есть\ RiskZ2 >; \\ \tilde{L}_3^{(1)} :< ЕСЛИ\ E_{24}\ ИЛИ\ E_{33}\ ИЛИ\ E_{34}\ ИЛИ\ E_{42}\ ИЛИ\ E_{43}\ ИЛИ\ E_{44}\ \text{ТО}\ risk_i\ есть\ RiskZ3 >; \\ \tilde{L}_4^{(1)} :< ЕСЛИ\ E_{51}\ ИЛИ\ E_{52}\ ИЛИ\ E_{53}\ ИЛИ\ E_{54}\ \text{ТО}\ risk_i\ есть\ RiskZ3 >; \end{cases}$$

где E_{kj} — высказывание вида: $<\rho_i$ есть α_{xl} и u_i есть $\alpha_{yj} >$.

В том случае если какой-либо из ДФ существенной среды $DF_i \in DF$ по значению своих параметров попадает в одну из потенциально «опасных» зон карты рисков, например во 2-ю и 3-ю зоны, то он помещается во множество «опасных» для ИС ДФ, защиту от которых необходимо предусмотреть до их наступления:

$$DangDF = \{DF\}(p,u,risk) \mid risk \in RiskZ2 \cup RiskZ3\}, DangDF \subseteq DF.$$

Далее формируется матрица отношений R^{DFRS} между потенциально опасными ДФ существенной среды DangDF⊆ DF и возможными катастрофоустойчивыми решениями, представленными множеством DRS, которые могут быть использованы организацией для повышения уровня катастрофоустойчивости системы.

В модели отношений определены следующие типы связей:

- МР — имеется катастрофоустойчивое решение, данный вид связи указывает, что для существующего «опасного» ДФ в ИС имеется средство, противодействующее данной угрозе;
- NMР — нет катастрофоустойчивого решения, данный вид связи показывает, что для существующего «опасного» ДФ существенной среды в ИС нет средства, осуществляющего защиту.

Отношение R^{DFRS}, задающее связи между катастрофоустойчивыми решениями в ИС *DRS* и множеством актуальных для данной ИС ДФ — *DangDF*, представлено в виде матрицы (2):

$$R^{DFRS} = \left| r_{ij}^{DFRS} \right|, \quad (2)$$

где r_{ij}^{DFRS} отображает наличие и тип связи между i-м «опасным» ДФ существенной среды и j-м катастрофоустойчивым решением.

При этом $i \in DangDF$, а $j \in DRS$, $r_{ij}^{DFRS} \in \{MP,\ NPM\}$, МР, NMР — наличие связи определенного типа между i-м «опасным» ДФ и j-м катастрофоустойчивым решением. Для элементов данной матрицы верно следующее:

$$r_{ij}^{DFRS} = \begin{cases} MP, если\ i\text{-е ДФ закрывается j-м катастрофоустойчивым решением} \\ NMP, если\ i\text{-е ДФ не закрывается j-м катастрофоустойчивым решением} \end{cases}$$

Если для всех значений i = k, $r_{ij}^{DFRS} = NMP$, то делается вывод о том, что в ИС нет защиты от деструктивного воздействия данной существенной среды и для повышения уровня катастрофоустойчивости ИС организации-владельцу необходимо внедрить дополнительные катастрофоустойчивые решения.

Заключение

Таким образом, при исследовании уровня катастрофоустойчивости ИС организации и обоснования необходимости внедрения того или иного класса катастрофоустойчивых решений необходимо в первую очередь выполнить следующие действия:

- определить множество ДФ существенной среды, актуальных для данной ИС, деструктивное воздействие которых может оказать влияние на работоспособность ИС в целом, непрерывность выполнения бизнес-процессов организации-владельца и целостность обеспечивающей инфраструктуры (макрообъекта): $DF_i \in DF, i = 1..n$;
- определить характеристики каждого ДФ, такие как вероятность реализации, потенциально возможный ущерб и риск;
- составить трехзонную карту рисков, в соответствии с которой выделить подмножество не допустимых по уровню риска ДФ существенной среды, защиту от которых путем подбора и внедрения соответствующих катастрофоустойчивых решений организация — владелец ИС должна обеспечить в первую очередь;
- в соответствии с построенной матрицей отношений выявить все не закрытые катастрофоустойчивыми решениями потенциально «опасные» для функционирования ИС ДФ существенной среды и

перейти к подбору группы наиболее эффективных и оптимальных по соответствию предъявляемым требованиям организацией — владельцем ИС катастрофоустойчивых решений.

Предложенный подход может применяться как в процессе создания и сопровождения реальных ИС, так и для моделирования и анализа различных вариантов построения ИС с целью поиска наиболее эффективного при вариации входных параметров. В качестве данных параметров могут выступать требования организации к уровню катастрофоустойчивости системы, катастрофы различного характера, которые могут оказать дестабилизирующее воздействие, а также определенное количество доступных ресурсов.

СПИСОК ЛИТЕРАТУРЫ:

1. Указание ЦБ РФ от 14 сентября 2011 г. № 2695-У «О требованиях к обеспечению бесперебойности осуществления перевода электронных денежных средств». URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=119777 (дата обращения: 20.03.2013).
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации». URL: http://base.garant.ru/12148555 (дата обращения: 10.03.2013).
3. Постановление Правительства РФ от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных систем к информационно-телекоммуникационным сетям». URL: http://base.garant.ru/195593 (дата обращения: 10.03.2013).
4. Приказ Минкомсвязи РФ от 25 августа 2009 г. № 104 «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования». URL: http://www.bestpravo.ru/federalnoje/hj-pravila/j4b.htm (дата обращения: 16.03.2013).
5. Приказ ФСБ/ФСТЭК от 31 августа 2010 г. № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования». URL: http://fstec.ru/normativnye-pravovye-akty-tzi/110-deyatelnost/tekush-chaya/tekhnicheskaya-zashchita-informatsii/normativnye-pravovye-akty/prikazy/370-prikaz-fstek-rossii-ot-31-avgusta-2010-g-n-489 (дата обращения: 16.03.2013).
6. Стандарт Банка России от 21 июня 2010 г. СТО БР ИББС–1.0.-2010 «Обеспечение информационной безопасности организации банковской системы Российской Федерации». URL: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf (дата обращения: 01.09.2013).
7. *Atkina V. S.* Semantic model of disaster recovery information system // European Science and Technology: international scientific conference. Wiesbaden, Germany. 2012. P. 162–164.