УДК 004.946; 330.342.24

РЕСУРСНЫЙ ПОДХОД К УПРАВЛЕНИЮ РИСКАМИ НЕЗАВИСИМОГО И СОВМЕСТНОГО ТЕСТИРОВАНИЯ РЕЛИЗОВ IT-СЕРВИСОВ

Киселева Т.В., Маслова Е.В.

Сибирский государственный индустриальный университет

Аннотация.
В настоящий век информационных технологий самым востребованным, следовательно, и самым дорогим товаром является информация. Ее порча, потеря, утечка, использование конкурирующей фирмой несут колоссальные убытки для организации, деятельность которой и так сопряжена с многочисленными рисками. Подверженность фирм в рыночной экономике рискам никогда не теряет актуальности, но в условиях экономического кризиса она становится особенно значимой, поскольку вероятность появления ущерба и уменьшения прибыли возрастает в разы. При помощи управления рисками можно добиться максимально возможной эффективности работы организации. За рубежом система управления рисками предприятия настолько развита, что ее используют предприятия даже в самых стабильных экономических условиях. Учитывая, каков уровень нестабильности российской экономики, то становится понятным, почему в нашей стране уделять большое внимание вопросам управления рисками крайне необходимо. В российской экономике вопросы управления рисками практически не привлекали внимания у руководителей российских предприятий вплоть до того момента, пока не настал глобальный финансовый кризис. На этом основании в статье рассмотрены вопросы управления рисками предприятия, связанными с использованием корпоративных информационных систем. Предложен авторский ресурсный подход к управлению рисками независимого и совместного тестирования релизов IT-сервисов. Представлен математический аппарат риск-менеджмента информационной среды современного предприятия…

Информация о статье
Принята 01 августа 2017

Ключевые слова: информационные риски, риск-менеджмент, IT-сервис, предприятие, российская экономика.

DOI: 10.26730/2587-5574-2017-2-33-46

RESOURCE APPROACH TO RISK MANAGEMENT OF INDEPENDENT AND JOINT TESTING OF IT-SERVICES RELEASES

Tamara V. Kiseleva, Elena V. Maslova

Siberian State industrial University

Abstract.
At present time when information technologies are dominating, the most popular and expensive good is the information. Its damage, loss, leakage, use by a competing firm incur enormous losses for the companies, which activities are already fraught with numerous risks. The firm's exposure to market risks never loses its relevance, but in the conditions of an economic crisis, it becomes especially significant because the likelihood of damage and loss of profits increases several times. With the help of risk management, you can achieve the highest possible efficiency of the organization. Abroad, the corporative risk management system is developed so much that it is used by enterprises even in the most stable economic conditions. Considering the level of Russian economy entropy it becomes clear why in this country paying much attention to risk management is extremely necessary. In the Russian economy, the issues of risk management hardly attracted attention from the leaders of Russian enterprises until the moment when the global financial crisis came. On this basis, the article describes the issues of enterprise risk management associated with the use of corporate information systems. The author's resource approach to risk management of independent and joint testing of IT services releases is offered. The mathematical apparatus of risk management of the information environment of a modern enterprise is presented.

Article info
Received August 01, 2017

Keywords:
information risks, risk management, IT-service, enterprise, Russian economy

Введение

В условиях выхода российской экономики на неоиндустриальный путь развития, сопровождающийся качественными изменениями ее структуры, значительным повышением доли IT-сектора в ВВП и экспорте [1-2], возрастает опасность недобросовестного использования информации, имеющей коммерческую ценность [3-4]. В связи с этим возрастает актуальность анализа методологии исследования рисков IT-сервисов.

Объекты и методы исследований

Риск – это возможная вероятность потерь, опасность неблагоприятного исхода какого-либо события, которое может произойти или не произойти, это степень опасности подвергнуться воздействию негативных событий и их возможных последствий.

Категории риска:

1. Риск, который можно исключить;
2. Риск, от которого можно застраховаться;
3. Риск, для которого необходимо создать профилактику.

В зависимости от возможного результата риски можно поделить на две категории: чистые и спекулятивные. Чистые риски – это возможность получения отрицательного или нулевого баланса. К ним относятся: природно-естественные, экологические, политические, транспортные, часть коммерческих.

Спекулятивные риски – это возможность получения как положительного, так и отрицательного результата. К ним относятся финансовые.

Степень риска – это вероятность наступления потерь и размер возможного ущерба. Основой риска является, прежде всего, неопределенность ситуации, т.е. неизвестность условий обстановки, окружающей ту или иную деятельность, и перспектив изменения этих условий. Чем больше неопределенность, тем больше степень риска. По сути, уровень риска – это произведение вероятности реализации угрозы на ущерб от нее [5].

Количественные характеристики любого вида риска A: вероятность P=P(A), ущерб U=U(A), опасность O=O(A)=P*U.

Риски, которым подвергается информация в процессе функционирования компании, выделяются в особую группу, так называемые информационные риски. И обеспечение информационной безопасности – одна из главнейших задач современного предприятия.

Информационные риски — это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий, т.е. эти риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи [5].

Риск-менеджмент (управление рисками; англ. Risk management) — процесс принятия и выполнения управленческих решений, направленных на снижение вероятности возникновения неблагоприятного результата и минимизацию возможных потерь, вызванных его реализацией.

Процесс управления рисками можно подразделить на следующие этапы [5]:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методики оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, определение уязвимостей в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Этапа 6 и 7 относятся к выбору защитных средств или нейтрализации рисков, а остальные – к оценке рисков.

Перечисление этих этапов показывает, что процесс управления рисками цикличен. По сути, последний этап – это оператор конца цикла, который говорит о том, что нужно вернуться к началу. Риски требуют постоянного контроля и периодической переоценки. При этом, добросовестно выполненная, хорошо документированная их первая оценка существенно упрощает последующие.

ISSN 2587-5574

Как правило, для любой компании важными являются абсолютно все составляющие, но все это невозможно включить в анализ, приходится останавливаться на некотором уровне детализации и отдавать себе отчет в его приблизительности. Также при анализе следует учитывать, в который раз он проводится. Если впервые, то предпочтительнее провести более полную оценку, если же анализ делается не в первый раз, можно ограничиться поверхностным его проведением.

При идентификации активов, т.е. всего того, что важно для организации и ее функционирования, следует учитывать не только материальные составляющие, но и такие компоненты информационной системы, как персонал, инфраструктуру, а также нематериальные ценности, например, репутацию компании. Для каждого актива должен быть определен его владелец, т.е. тот, кто за него отвечает.

Далее определяется критичность активов, т.е. величина потенциального ущерба организации в случае нарушения требований информационной безопасности, что является наиболее сложным процессом. Оценка критичности выполняется в зависимости от влияния рисков на три параметра активов: конфиденциальность, целостность и доступность.

Риск появляется в случае потенциальной угрозы, а ее присутствие объясняется наличием уязвимости в защите информационных систем. Уязвимость характеризуется слабостью защиты, наличием условий, позволяющим угрозе причинить ущерб.

Сначала необходимо идентифицировать все имеющиеся угрозы, исходя из соображений здравого смысла, но при этом провести их максимально полное рассмотрение. Часто считается целесообразным выявление еще и источников возникновения угроз, поскольку это поможет при выборе средств защиты.

Далее оценивается вероятность ее осуществления и размер возможного ущерба. Все это можно сделать, используя качественную шкалу. Размер ущерба от реализации угрозы зависит от стоимости ресурса, который подвергается риску и от степени разрушительности воздействия на ресурс, выражаемой в виде коэффициента разрушительности.

После реализации всех этих этапов необходимо приступить непосредственно к оценке рисков.

Для оценки рисков часто применяется самый простой метод – умножение вероятности осуществления угрозы на возможный ущерб. Полученный результат приводится к качественной шкале, по которой и оценивается приемлемость риска.

На следующем этапе выбираются защитные меры (контрмеры) и оценивается их стоимость. При этом нужно учитывать не только прямые расходы на приобретение нового оборудования, но и на обучение персонала. Если контрмера экономически выгодна, ее оставляют на рассмотрение, если же нет, то не следует ее сразу сбрасывать со счетов, потому что все сделанные до этого расчеты были приблизительны и на практике расходы могут оказаться не такими большими, или ущерб будет значительно выше, чем предполагалось.

После того, как выбраны меры защиты, их внедряют, а затем проверяют на работоспособность. Если остаточный риск приемлем, то можно назначать дату ближайшей переоценки, если же нет, то весь комплекс анализа и оценки проводится заново.

Одной из актуальных проблем в работе многих современных предприятий становится вопрос управления ИТ-деятельностью организаций, в основе которого лежит понятие модели жизненного цикла ИТ-сервиса. Не менее важным является обеспечение информационной безопасности.

ИТ-сервис – это комплекс взаимодействующих ИТ-активов, цель которого состоит в производстве ценности для потребителя, определяемой полезностью, доступностью, мощностью, непрерывностью и безопасностью сервиса [6]. Таким образом, ИТ-сервис – это совокупность активов, т.е. всем тем, чем располагает организация для производства сервиса. Они могут быть управленческими, информационными, организационными, финансовыми, инфраструктурными и т.д., также это могут быть знания, приложения, процессы, проекты.

ИТ-сервис обладает такими свойствами, как полезность и применимость, которым присущи определенные характеристики. Свойство полезности сервиса выражает положительный эффект от его внедрения для заказчика, так как помогает достичь желаемой цели. Полезность характеризуется следующими результатами:

1. Первичным – это конкретная форма представления непосредственного результата;
2. Подсистемным – планируемый эффект;

3. Общесистемным – экономические, социально-экономические и политические эффекты.

Свойство применимости говорит о том, что ИТ-сервис доступен в нужное время в достаточном объеме. Применимость обладает:

1. Доступностью – способность выполнить свою функцию в согласованное время;
2. Мощностью – производительность сервиса;
3. Непрерывностью – способность обеспечить деятельность заказчика при возникновении форс-мажорных обстоятельств;
4. Безопасностью – уровень защиты сервиса от рисков.

На рисунке 1 представлена модель жизненного цикла ИТ-сервиса. В соответствие со стандартом ISO 9004-1 жизненный цикл изделия (ЖЦИ) — совокупность взаимосвязанных процессов, выполняемых от момента выявления потребностей в определенном продукте (услуге) до момента удовлетворения этих потребностей и утилизации продукта (услуги) [6].

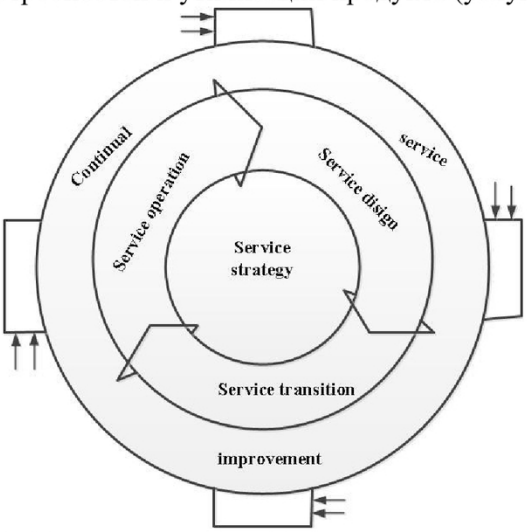

Рис. 1. Жизненный цикл ИТ-сервиса по версии ITIL

Согласно ITIL (библиотеке лучших руководств по управлению ИТ-сервисами) жизненный цикл ИТ-сервиса включает следующие стадии:

1. Стратегия.
2. Проектирование.
3. Внедрение.
4. Эксплуатация.

В работе [6] рассматривается также стадия вывода сервиса из эксплуатации или стадия утилизации сервиса. Рассмотрим эти стадии более подробно.

На стадии стратегии проводится SWOT-анализ ИТ-организации, т.е. выявляются ее сильные и слабые стороны, ее возможности и угрозы, определяются ее миссия, перспективы, планы и т.д. ИТ-провайдер, т.е. тот, кто обеспечивает заказчика ИТ-сервисами, должен определить свои возможности, а также требования к разрабатываемому ИТ-сервису, оценить его востребованность на рынке в данный момент. В конце этой стадии вырабатывается технико-экономическое обоснование необходимого сервиса.

Следующие две стадии – самые важные, а значит, они подвержены риску больше всего. На стадии проектирования разработанная на предыдущем этапе стратегия реализуется за счет создания новых и/или изменения имеющихся сервисов.

Сформированный на стадии проектирования сервис далее внедряется в эксплуатационную среду. Под этим понимается развертывание сервиса в системе, его тестирование, обучение персонала работе, а также создание условий для работоспособности сервиса и восстановительных процедур. При этом происходит изменение эксплуатационной среды, в результате чего возникает риск ее полного или частичного разрушения.

ISSN 2587-5574

На стадии эксплуатации начинается повседневное применение спроектированного и внедренного ИТ-сервиса в работе организации. Заказчик может оценить реальное качество как самого сервиса, так и поддержки, осуществляемой ИТ-провайдером.

Постоянная эксплуатация сервиса приводит к тому, что его полезность снижается или увеличивается стоимость поддержания его в работоспособном состоянии. Тогда руководством принимается решение о целесообразности дальнейшей работы с ним. Также списать и утилизировать сервис возможно в случае отказа клиентов его использовать. На стадии утилизации сервиса освобождаются соответствующие активы, обновляются портфель сервисов, база данных конфигураций и база знаний.

На любой из вышеперечисленных стадий жизненного цикла могут возникнуть какие-либо риски, в том числе и информационные. Для их уменьшения или предотвращения рекомендуется проводить периодические анализ и оценку, на основе которых можно выработать защитные контрмеры.

Результаты и их обсуждение

Как уже было сказано выше, наиболее подверженными риску являются стадии проектирования и внедрения. В частности, к таким рискам могут относиться небрежное проектирование, отказ инфраструктуры, отказ функционирования оборудования, человеческие ошибки и некомпетентность, а также различные форс-мажорные обстоятельства.

В процессе внедрения новой версии ИТ-сервиса может возникнуть риск потери самой эксплуатационной среды. Для снижения риска как разрушения среды, так и потери внедряемого ИТ-сервиса предлагается разбить множество тестируемых сервисов на релизы (это совокупность активов, которые внедряются в эксплуатационную среду за один прием), встраивать их в тестовую эксплуатационную среду и проводить предварительное независимое или совместное тестирование. В случае независимого тестирования релизы последовательно друг за другом встраиваются в эксплуатационную среду и поочередно тестируются. При системном тестировании релизы ИТ-сервиса встраиваются совместно. Чем выше качество проведенного тестирования, тем меньше вероятность возникновения какого-либо инцидента во время эксплуатации ИТ-сервиса.

Но для построения тестовой среды и проведения тестирования требуются средства, которые предполагают дополнительные затраты, что может быть оправдано в случае, если необходимые ресурсы существенно превышают потери ИТ-провайдера и заказчиков ИТ-сервиса при реализации возможных рисков. Следовательно, перед лицом, принимающим решения, и проводящим тестирование стоит задача минимизации затрат, необходимых при внедрении релизов ИТ-сервисов в эксплуатационную среду.

Ниже на рисунке 2 приведена схема изменения текущих базовых состояний эксплуатационной среды на новые состояния в результате встраивания в среду релизов ИТ-сервиса, обновляющих технологические активы (релиз A_1), активы приложений (релиз A_2), активы портфеля сервисов (релиз A_3) и активы бизнеса (релиз A_4) [7].

Обозначим через $P(A_i), i=\overline{1,n}$ – вероятности возникновения ИТ-происшествий в эксплуатационной среде при встраивании соответствующего релиза после тестирования. Вероятности, характеризующие качество проектирования релизов ИТ-сервисов, будем считать известными или заданными. Качество К тестирования будем оценивать по трехбалльной шкале измерения: 1 – «плохо», что соответствует большому риску возникновения ИТ-происшествий, 2 – «удовлетворительно», что соответствует среднему риску, 3 – «хорошо», что соответствует малому риску.

Обозначим затраты на тестирование релиза A_i через $z(A_i), i=\overline{1,n}$. Будем считать заданными функции затрат от качества тестирования релизов $z_K(A_i), K=\overline{1,3}, i=\overline{1,n}$, что представлено в таблице 1.

Таблица 1. Функции затрат в зависимости от качества тестирования релизов

$K(A_i)$	3	2	1
$z_K(A_i)$	$z_3(A_i)$	$z_2(A_i)$	$z_1(A_i)$

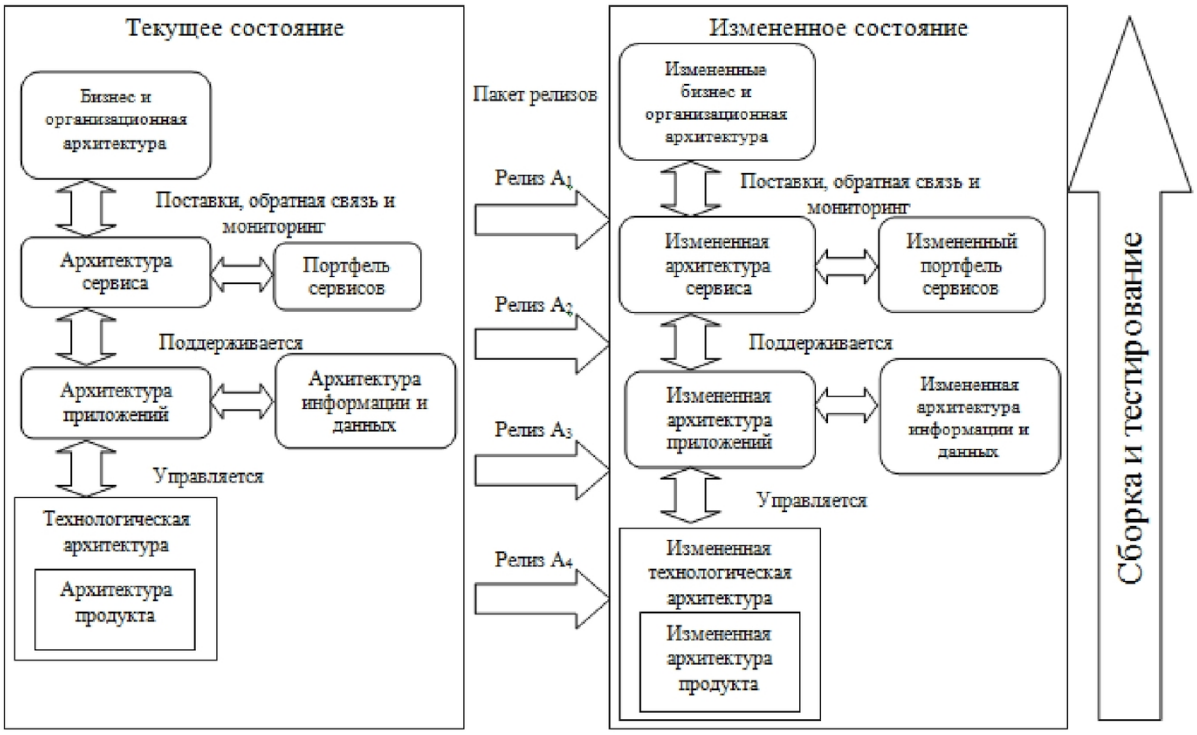

Рис.2. Изменения текущих базовых состояний ИТ-среды на новые базовые состояния

Дадим постановку задачи оптимального распределения ресурсов при независимом и системном тестировании релизов ИТ-сервисов [7-8].

Дано:

1. Эксплуатационная среда, состав которой для 4-х релизов показан на рис. 1.

2. Пакет релизов $A_i, i = \overline{1,n}$.

3. Качество тестирования релизов *K*.

4. Вероятности возникновения ИТ-происшествий $P(A_i), i = \overline{1,n}$.

5. Затраты на тестирование релизов: $z_K(A_i), K = \overline{1,3}, i = \overline{1,n}$.

6. Ограничение: $K(A_1 \cup A_2 \cup ... \cup A_n) \geq K^*$ при независимом тестировании ИТ-сервиса или $K(A_n | A_1, A_2, ..., A_{n-1}) \geq K^*$ при совместном тестировании ИТ-сервиса.

7. Критерий: суммарные затраты на тестирование релизов: $\sum_{i=1}^{n} z_K(A_i)$.

Требуется: оптимизировать распределение ресурсов на тестирование при соблюдении ограничения и минимизации критерия, т.е. $\sum_{i=1}^{n} z_K(A_i) \to \min$. Иначе, требуется определить такие минимальные затраты $z_K(A_i), K = \overline{1,3}, i = \overline{1,n}$, которые обеспечивают качество $K(A_1 \cup A_2 \cup ... \cup A_n) \geq K^*$ при независимом тестировании ИТ-сервиса или $K(A_n | A_1, A_2, ..., A_{n-1}) \geq K^*$ при совместном тестировании релизов ИТ-сервиса, где К* - заданное качество.

Для решения этой задачи предлагается использовать метод сетевого (дихотомического) программирования, описанного в работе [9] с целью упрощения процедуры решения. Согласно этому методу сложные функции представляются в виде композиции (суперпозиции) более простых функций. Графическое представление этого способа – это сетевой граф, в котором входы – переменные функций, выходы – сами функции, последующие вершины – это функции, входящие в композицию. Такое представление называется сетевым.

Необходимым условием для применения метода сетевого программирования является структурное подобие двух функций. Две функции являются структурно подобными в том случае, если их сетевые представления совпадают.

ISSN 2587-5574

Рассмотрим структуру, приведенную на рис. 3 и описывающую сетевые представления функции затрат для проведения тестирования и функции вероятности реализации инцидентов при этом. Очевидно, что сетевые представления функций одинаковы, следовательно, эти функции структурно подобны, а значит применение метода сетевого программирования возможно.

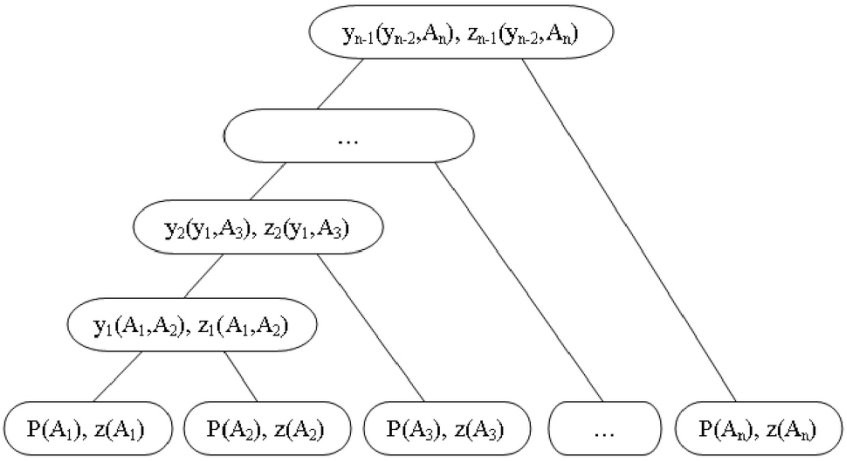

Рис. 3. Сетевое представление функций $P(A_i)$ и $z(A_i)$

Сначала рассматриваем затраты на тестирование релизов A_1 и A_2 и вероятности возникновения инцидентов при внедрении этих релизов в ИТ-среду. Их совместную вероятность обозначим через $y_1(A_1, A_2)$, а затраты – через $z_1(A_1, A_2)$. Далее к y_1 и z_1 присоединяем затраты, необходимые для тестирования релиза A_3, и вероятность возникновения при этом ИТ-происшествий. Получаем соответственно затраты z_2 и вероятность y_2. Аналогично рассчитываются вероятности и затраты на всех последующих шагах до получения значения вероятности y_{n-1} и затрат z_{n-1} при подсоединение релиза A_n.

Приведем решение задачи оптимального распределения ресурсов сначала для случая системного тестирования релизов ИТ-сервисов при их внедрении в эксплуатационную среду.

Внедряемый ИТ-сервис S состоит в общем случае из n релизов A_i, т.е. $S=(A_1, A_2, \dots A_n)$. Вероятность $P(S)=P(A_1, A_2, \dots A_n)$ возникновения различных инцидентов при внедрении сервиса связана с числом связей, которые проходят проверку в эксплуатационной среде.

Согласно теореме умножения вероятностей [10], вероятность возникновения инцидентов будет рассчитываться по формуле:

$$P(A_1, A_2, ..., A_n) = P(A_1)P(A_2 \mid A_1).....P(A_n \mid A_1, A_2, ..., A_{n-1}). \quad (1)$$

Приведем граф, который описывает связи между четырьмя релизами с компонентами самой среды, при этом числа на ветвях графа – это количества связей релизов между собой и со средой (рис. 4).

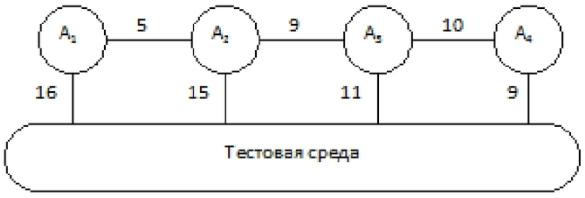

Рис.4. Взаимные связи сервисов и их связи с эксплуатационной средой

В таблице 2 приведен пример числовых значений взаимных связей четырех релизов ИТ-сервисов и связей с эксплуатационной средой.

Таблица 2. Численные значения связей сервисов

	A_1	A_2	A_3	A_4
A_1	16	5	0	0
A_2	5	15	9	0
A_3	0	9	11	10
A_4	0	0	10	9

Положим, что:

$$P(A_i \mid A_1, A_2, ..., A_{i-1}) = \frac{A_{ii} + A_{i(i-1)}}{\sum_{i=1}^{n}(A_{ii} + A_{i(i-1)})}, \quad (2)$$

где $A_{10}=0$.

Тогда:

$$P(A_1, A_2, ..., A_n) = \prod_{i=1}^{n}\left(\frac{A_{ii} + A_{i(i-1)}}{\sum_{i=1}^{n}(A_{ii} + A_{i(i-1)})}\right). \quad (3)$$

Интервал $(0 \div P(A_i \mid A_1, A_2, \ldots, A_{i-1}))$ разбивается на три равных подинтервала. После этого оценивается качество тестирования в зависимости от значения вероятности тестирования. Функции затрат $z_K(A_i \mid A_1, A_2, ..., A_{i-1}), K = \overline{1,3}, i = \overline{1,n}$ от качества тестирования релизов при этом считаются известными.

Для функции затрат в этом случае имеют место следующие соотношения:

$$\begin{aligned} &z_1 = \sum_{i=1}^{2} z(A_i); \\ &z_2 = z_1 + z(A_3); \\ &\ldots \\ &z_{n-1} = z_{n-2} + z(A_n). \end{aligned} \quad (4)$$

Для вероятностей справедливы следующие соотношения:

$$\begin{aligned} &y_1 = P(A_1); \\ &y_2 = P(A_1)P(A_2 \mid A_1); \\ &\ldots; \\ &y_{n-1} = P(A_1)P(A_2 \mid A_1)\ldots P(A_n \mid A_1, \ldots, A_{n-1}). \end{aligned} \quad (5)$$

Для решения исходной задачи методом сетевого программирования необходимо последовательно решить (n-1) задач:

Задача первого уровня:

$$\begin{aligned} &z_1 = \sum_{i=1}^{2} z(A_i) \to \min; \\ &K(y_1) = K(P(A_1)P(A_2 \mid A_1)) \geq K^*. \end{aligned} \quad (6)$$

Задача второго уровня:

$$\begin{aligned} &z_2 = z_1 + z(A_3) \to \min; \\ &K(y_2) = K(P(A_1)P(A_2 \mid A_1)P(A_3 \mid A_1, A_2)) \geq K^*. \end{aligned} \quad (7)$$

…

Последней (n-1) задачей решается задача, которая соответствует выходу из сети:

$$\begin{aligned} &z_{n-1} = z_{n-2} + z(A_n); \\ &K(y_{n-1}) = K(P(A_1)P(A_2 \mid A_1)\ldots P(A_n \mid A_1, \ldots, A_{n-1})) \geq K^*. \end{aligned} \quad (8)$$

Решение (n-1) задачи является решением исходной задачи.

В случае независимого тестирования релизов ИТ-сервисов вероятность возникновения ИТ-происшествий рассчитывается по-другому.

Сетевое представление функций затрат и вероятностей возникновения при таком виде тестирования аналогично сетевому представлению, рассмотренному выше. Затраты в этом случае также рассчитываются по формуле (4).

Вероятность суммы двух совместных событий A и B определяется по формуле [10]:

$$P(A + B) = P(A) + P(B) - P(AB). \quad (9)$$

Для решения задачи оптимального распределения ресурсов на тестирование релизов, как и в предыдущей задаче, ее следует разбить на несколько подзадач. Вероятности y_i возникновения ИТ-происшествий рассчитываются по формулам:

$$y_1(A_1, A_2) = P(A_1 + A_2) = P(A_1) + P(A_2) - P(A_1 \cap A_2), \quad (10)$$

$$y_2(y_1, A_3) = P(A_1 + A_2 + A_3) = y_1 + P(A_3) = y_1 + P(A_3) - y_1 P(A_3), \quad (11)$$

…

$$y_{n-1}(y_{n-2}, A_n) = P(A_1 + \ldots + A_n) = y_{n-2} + P(A_n) - y_{n-2}P(A_n). \quad (12)$$

ISSN 2587-5574

Сначала рассчитываются значения $y_1(A_1, A_2)$ и $z_1(A_1, A_2)$. При этом

$$z_1 = \sum_{i=1}^{2} z(A_i) \to \min, \quad K(y_1) = K(A_1 + A_2) \geq K^*. \tag{13}$$

Далее с использованием полученных значений находятся $y_2(y_1, A_3)$; $z_2(y_1, A_3)$, при следующих условиях:

$$z_2 = z_1 + z(A_3) \to \min, \quad K(y_2) = K(A_1 + A_2 + A_3) \geq K^*. \tag{14}$$

…

Последними аналогично рассчитываются значения $y_{n-1}(y_{n-2}, A_n)$; $z_{n-1}(y_{n-2}, A_n)$ при условиях:

$$z_{n-1} = z_{n-2} + z(A_n) \to \min, \quad K(y_{n-1}) = K(A_1 + \ldots + A_n) \geq K^*. \tag{15}$$

Это и является решением исходной задачи.

В случае с тестированием четырех релизов, связи которых приведены на рисунке 4 и в таблице 2, по формуле 2 получаем:

$$P(A_1) = \frac{16+0}{(16+0)+(15+5)+(11+9)+(9+10)} = \frac{16}{75} = 0{,}21;$$

$$P(A_2 \mid A_1) = \frac{15+5}{(16+0)+(15+5)+(11+9)+(9+10)} = \frac{20}{75} = 0{,}27; \tag{16}$$

$$P(A_3 \mid A_1, A_2) = \frac{11+9}{(16+0)+(15+5)+(11+9)+(9+10)} = \frac{20}{75} = 0{,}27;$$

$$P(A_4 \mid A_1, A_2, A_3) = \frac{9+10}{(16+0)+(15+5)+(11+9)+(9+10)} = \frac{19}{75} = 0{,}25.$$

Пусть затраты на тестирование релизов A_1 и A_2 в зависимости от качества проводимого тестирования описываются функциями $z_K(A_i)$, их значения заданы и приведены в таблицах 3 и 4. Кроме этого, вычисленные интервалы $P(A_i)$ делятся на три равных подинтервала.

Таблица 3. Значения затрат $z_K(A_1)$ при различных интервалах вероятностей и показателях качества тестирования

$K(P(A_1))$	3	2	1
$P(A_1)$	(0 ÷ 0,07)	(0,07 ÷ 0,14)	(0,14 ÷ 0,21)
$z_K(A_1)$	15	12	8

Таблица 4. Значения затрат $z_K(A_2|A_1)$ при различных интервалах вероятностей и показателях качества тестирования

$K(P(A_2\|A_1))$	3	2	1
$P(A_2\|A_1)$	(0 ÷ 0,09)	(0,09 ÷ 0,18)	(0,18 ÷ 0,27)
$z_K(A_2\|A_1)$	21	17	9

Перемножая значения середин каждых полученных интервалов $P(A_1)$ и $P(A_2|A_1)$ при соответствующих значениях качества, получаем значения вероятности y_1. Затраты, необходимые для тестирования, вычисляются путем суммирования затрат $z_K(A_1)$ и $z_K(A_2|A_1)$. Эти результаты приведены в таблице 5.

Таблица 5. Значения вероятностей y_1 и затрат $z(y_1)$ в зависимости от качества тестирования релизов

$K(P(A_1))$	3	3	3	2	2	2	1	1	1
$K(P(A_2\|A_1))$	3	2	1	3	2	1	3	2	1
y_1	0,0016	0,0047	0,079	0,0047	0,0141	0,0236	0,0079	0,0236	0,0394
$z(y_1)$	36	32	24	33	29	21	29	25	17

Далее интервал $(0 \div \max(y_1))$ делится так же на три равных подинтервала, проверяется вхождение каждого полученного значения вероятности в эти интервалы. В качестве результата из

каждого интервала выбирается то значение вероятности, при котором затраты будут минимальными. Таким образом, получено решение задачи первого уровня, что приведено в таблице 6.

Далее рассчитываем значения вероятности возникновения инцидентов и затрат на тестирование релизов A_1 и $(A_2|A_1)$ с релизом A_3. y_1 и $z(y_1)$ вычислены на предыдущем шаге, $P(A_3|\ A_2,A_1)$ и $z_K(A_3|A_2,A_1)$ известны заранее, их значения приведены в таблице 7.

Таблица 6. Итоговые значения вероятностей и затрат на тестирование релизов (A_1) и $(A_2|A_1)$

$K(y_1)$	3	2	1
y_1	0,0079	0,0141	0,0394
$z_K(y1)$	24= $=z_3(A_1)+z_1(A_2\|A_1)$	29= $=z_2(A_1)+z_2(A_2\|A_1)$	17= $=z_1(A_1)+z_1(A_2\|A_1)$

Таблица 7. Значения затрат $z_K(A_3|\ A_2,A_1)$ при различных интервалах вероятностей и показателях качества тестирования

$K(P(A_3\|\ A_2,A_1))$	3	2	1
$P(A_3\|\ A_2,A_1)$	(0 ÷ 0,09)	(0,09 ÷ 0,18)	(0,18 ÷ 0,27)
$z_K(A_3\|\ A_2,A_1)$	22	19	11

Расчет значений вероятности y_2 и затрат $z(y_2)$ проводится аналогично вышеизложенному, то есть решается задача второго уровня, ее результат приведен в таблицах 8 и 9.

Таблица 8. Значения затрат $z(y_2)$ и вероятности y_2 при различном качестве тестирования

$K(y_1)$	3	3	3	2	2	2	1	1	1
$K(P(A_3\|A_2,A_1))$	3	2	1	3	2	1	3	2	1
y_2	0,0004	0,0011	0,0018	0,0006	0,0019	0,0032	0,0014	0,0041	0,0068
$z(y_2)$	46	43	35	51	48	40	39	36	28

Таблица 9. Итоговые значения вероятности возникновения инцидентов при тестировании релиза $(A_3|A_2,A_1)$ и необходимых для этого затрат

$K(y_2)$	3	2	1
y_2	0,0014	0,0041	0,0068
$z_K(y_2)$	39= $=z_1(y_1)+z_3(A_3\|A_2,A_1)$	36= $=z_1(y_1)+z_2(A_3\|A_2,A_1)$	28= $=z_1(y_1)+z_1(A_3\|A_2,A_1)$

Далее аналогично рассчитываются значения вероятности и затраты на тестирование релиза A_4. Вероятности возникновения инцидентов и затраты на тестирование релиза A_4 описываются функциями $P(A_4|A_3,A_2,A_1)$ и $z_K(A_4|A_3,A_2,A_1)$, их значения приведены в таблице 10.

Таблица 10. Значения затрат $z_K(A_4|A_3,A_2,A_1)$

$K(P(A_4\|A_3,A_2,A_1))$	3	2	1
$P(A_4\|A_3,A_2,A_1)$	(0 ÷ 0,08)	(0,08 ÷ 0,16)	(0,16 ÷ 0,25)
$z_K(A_4\|A_3,A_2,A_1)$	15	10	8

По аналогии с прошлыми расчетами вычисляем вероятности реализации рисков и затраты, необходимые при системном тестировании релизов с релизом A_4. Все результаты приведены в таблицах 11 и 12.

Таблица 11. Значения вероятностей возникновения инцидентов y_3 и затрат $z(y_3)$

$K(y_2)$	3	3	3	2	2	2	1	1	1
$K(P(A_4\|A_3,A_2,A_1))$	3	2	1	3	2	1	3	2	1
y_3	0,000 06	0,000 20	0,000 29	0,000 16	0,000 49	0,000 86	0,000 27	0,000 81	0,0013 94
$z_K(y_3)$	54	49	47	51	46	44	43	38	36

ISSN 2587-5574

Таблица 12. Итоговые значения вероятности возникновения инцидентов и затрат на тестирование релиза ($A_4|A_3,A_2,A_1$)

$K(y_3)$	3	2	1
y_3	0,00027	0,00086	0,001394
$z_K(y_3)$	43= $=z_1(y_2)+z_3(A_4\|A_3,A_2,A_1)$	44= $=z_2(y_2)+z_1(A_4\|A_3,A_2,A_1)$	36= $=z_1(y_2)+z_1(A_4\|A_3,A_2,A_1)$

Следовательно, минимальные затраты на тестирование ИТ-сервиса с наилучшей оценкой качества тестирования, соответствующей 3 («хорошо»), составляют 43 единицы ресурсов, а вероятность возникновения инцидентов при внедрении сервиса ничтожно мала и составляет 0,00027.

Далее приведем пример решения задачи оптимального распределения ресурсов при независимом тестировании этих же четырех релизов, используя значения вероятностей возникновения инцидентов, рассчитанные для случая системного тестирования четырех релизов (формула (16)), а также значения затрат, необходимых для проведения тестирования. Аналогично оценивается качество проведения тестирования в зависимости от значений вероятностей возникновения инцидентов, а интервалы $(0 \div P(A_i))$ разбиваются на три равных подинтервала. Значения функций затрат $z(A_i)$ известны. Заданные значения затрат, вероятностей и качества тестирования при внедрении релизов A_1 и A_2 приведены в таблицах 13 и 14. В зависимости от качества тестирования релизов A_1 и A_2, а значит и вероятностей возникновения инцидентов при внедрении этих релизов рассчитываются вероятности y_1 и затраты $z(y_1)$, причем вероятности возникновения ИТ-происшествий при внедрении релиза на каждом интервале берутся максимальными. y_1 рассчитывается по формуле (10), $z(y_1)$ – по формуле (4).

Таблица 13. Значения затрат $z_K(A_1)$ при различных интервалах вероятностей и показателей качества тестирования

$K(P(A_1))$	3	2	1
$P(A_1)$	$(0 \div 0{,}07)$	$(0{,}07 \div 0{,}14)$	$(0{,}14 \div 0{,}21)$
$z_K(A_1)$	15	12	8

Таблица 14. Значения затрат $z_K(A_2)$ при различных интервалах вероятностей и показателей качества тестирования

$K(P(A_2))$	3	2	1
$P(A_2)$	$(0 \div 0{,}09)$	$(0{,}09 \div 0{,}18)$	$(0{,}18 \div 0{,}27)$
$z_K(A_2)$	21	17	9

Таблица 15. Значения вероятностей возникновения инцидентов при тестировании релизов A_1, A_2 и затрат, необходимых для этого, в зависимости от качества тестирования

$K(P(A_1))$	3	3	3	2	2	2	1	1	1
$K(P(A_2))$	3	2	1	3	2	1	3	2	1
y_1	0,154	0,237	0,321	0,217	0,295	0,372	0,281	0,352	0,423
$z(y_1)$	36	32	24	33	29	21	29	25	17

Следовательно, был получен интервал вероятностей $y_1 = (0{,}154 \div 0{,}423)$, который, в свою очередь, делится на три равных подинтервала, и качество тестирования релизов A_1 и A_2 приводится к трехбалльной шкале измерения. Для каждого подинтервала выбирается значение вероятности y_1 такое, что затраты на тестирование при этом минимальны. Если таких значений несколько, то выбирается минимальная вероятность y_1. Окончательное решение задачи первого уровня приведено в таблице 16.

Таблица 16. Итоговые значения y_1 и $z(y_1)$

$K(y_1)$	3	2	1
y_1	0,237	0,321	0,423
$z(y_1)$	32= $= z_3(A_1)+ z_2(A_2)$	24= $= z_3(A_1)+ z_1(A_2)$	17= $= z_1(A_1)+ z_1(A_2)$

Далее аналогично решается задача второго уровня, значения затрат, вероятностей при различном качестве тестирования при внедрении релиза A_3 заданы заранее, они приведены в таблице 17. С учетом этих данных, а также рассчитанных при решении задачи первого уровня значения затрат $z(y_1)$ и вероятностей возникновения инцидентов y_1 рассчитываются значения вероятностей y_2 возникновения инцидентов при внедрении релиза A_3 по формуле (11) и затрат $z(y_2)$, необходимых для этого.

Таблица 17. Значения затрат $z_K(A_3)$ при различных интервалах вероятностей и показателей качества тестирования

$K(P(A_3))$	3	2	1
$P(A_3)$	(0 ÷ 0,09)	(0,09 ÷ 0,18)	(0,18 ÷ 0,27)
$z_K(A_3)$	22	19	11

Таблица 18. Значения вероятностей y_2 и затрат $z(y_2)$

$K(y_1)$	3	3	3	2	2	2	1	1	1
$K(P(A_3))$	3	2	1	3	2	1	3	2	1
y_2	0,306	0,375	0,443	0,382	0,443	0,504	0,475	0,527	0,579
$z(y_2)$	54	51	43	46	43	35	39	36	28

Аналогично предыдущему шагу был получен интервал y_2=(0,306÷0,579), который делится на три равных подинтервала, на каждом подинтервале выбирается такое значение вероятности, при котором значение функции затрат минимально. Полученное решение задачи второго уровня приводится в таблице 19.

Таблица 19. Итоговые значения y_2 и $z(y_2)$

$K(y_2)$	3	2	1
y_2	0,382	0,443	0,579
$z(y_2)$	46= $= z_2(y_1)+ z_3(A_3)$	43= $= z_2(y_1)+ z_2(A_3)$	28= $= z_1(y_1)+ z_1(A_3)$

Следующей является задача третьего уровня, на котором рассчитываются значения вероятностей возникновения ИТ-инцидентов y_3 и затрат $z(y_3)$, необходимых для проведения тестирования релизов ИТ-сервиса. В приведенном примере задача третьего уровня является последней, для ее решения используются значения вероятностей y_2 возникновения инцидентов при внедрении релиза A_3 и затрат $z(y_2)$, рассчитанные на предыдущем шаге, а также заданные заранее значения затрат z_4 на тестирование релиза A_4 и вычисленные значения вероятности возникновения инцидентов при этом $P(A_4)$. Эти значения, а также рассчитанные с их помощью значения y_3 и $z(y_3)$, приведены в таблицах 20 и 21.

Таблица 20. Значения затраты $z_K(A_4)$

$P(A_4)$	(0 ÷ 0,08)	(0,08 ÷ 0,16)	(0,16 ÷ 0,25)
$K(P(A_4))$	3	2	1
$z_K(A_4)$	15	10	8

Таблица 21. Значения вероятностей y_3 затрат и $z(y_3)$

$K(y_2)$	3	3	3	2	2	2	1	1	1
$K(P(A_4))$	3	2	1	3	2	1	3	2	1
y_3	0,438	0,493	0,549	0,493	0,543	0,594	0,617	0,655	0,693
$z(y_3)$	61	56	54	58	53	51	43	38	36

Аналогично предыдущим шагам полученный интервал $y_3 = (y_{min} \div y_{max})$ делится на три подинтервала, из каждого выбирается такое значение y_3, при котором затраты будут минимальными. Этот результат представлен в таблице 22.

ISSN 2587-5574

Таблица 22. Итоговые значения y_3 и $z(y_3)$

$K(y_3)$	3	2	1
y_3	0,493	0,594	0,693
$z(y_3)$	56= $= z_3(y_2)+ z_2(A_4)$	51= $= z_3(y_2)+ z_1(A_4)$	36= $= z_1(y_2)+ z_1(A_4)$

В таблице 22 представлено окончательное решение исходной задачи. То есть минимальные затраты на тестирование ИТ-релиза с оценкой «хорошо» составляют 56 единиц ресурсов. При этом вероятность возникновения ИТ-происшествий при внедрении ИТ-сервиса равна 0,493.

После окончательного решения задач оптимизации распределения ресурсов, необходимых для проведения независимого и совместного тестирования релизов ИТ-сервисов при их внедрении в эксплуатационную среду было проведено сравнение этих двух видов тестирований. Установлено, что проведение совместного тестирования релизов для ИТ-провайдера целесообразнее, поскольку при одинаковых начальных условиях и наилучшем качестве тестирования вероятность реализации каких-либо рисков в процессе внедрения новых рабочих версий ИТ-сервисов или во время их эксплуатации в этом случае существенно меньше, чем при проведении независимого тестирования.

Заключение

Таким образом, в статье были рассмотрены основы управления информационными рисками, даны основные определения, связанные с ИТ-деятельностью предприятия. Кроме этого, была поставлена и решена задача оптимального распределения ресурсов при независимом и системном тестировании релизов ИТ-сервисов. Для упрощения процедуры ее решения предлагается использовать метод сетевого программирования. На конкретных примерах подробно рассмотрено решение этой задачи и проведен сравнительный анализ двух видов тестирований. На основе полученных при решении задачи результатов обосновано преимущество применения системного тестирования релизов ИТ-сервисов перед независимым.

Список источников

1. Доценко Е.Ю., Жиронкина О.В., Агафонов Ф.В., Генин А.Е. Роль конвергентных технологий в становлении непрерывного благополучия в неоиндустриальной экономике // Путеводитель предпринимателя. - 2016. - № 32.- С. 65-79.

2. Жиронкин С.А., Жиронкина О.В. Институциональные меры структурных преобразований экономики Кемеровской области // Известия Байкальского государственного университета. - 2013. - № 4. - С. 5-10.

3. Нуфер Л.П., Прокудина М.Д. Внутренний контроль как фактор борьбы с легализацией доходов, полученных преступным путём // Сборник статей международной научно-практической конференции «Проблемы и перспективы развития науки в России и мире», Екатеринбург, 2017. – Уфа: Изд-во «Аэтерна», 2017. - С. 132-136.

4. Нуфер Л.П., Прокудина М.Д. Противодействие легализации доходов, полученных преступным путём, и внутренний контроль в банке // Экономика и предпринимательство. - 2017. - № 1(78). - С.730-734.

5. Киселева Т.В., Маслова Е.В. Анализ информационных рисков / Моделирование, программное обеспечение и наукоемкие технологии в металлургии: сб. науч. тр. - Новокузнецк: изд. Сибирского гос. индустр. ун-та, 2011. - С. 75-80.

6. Зимин В.В. Механизмы декомпозиционного управления жизненным циклом информационно-технологических сервисов (на примере предприятий черной металлургии): Автореф. дис. … докт. техн. наук: 05.13.01. – Томск: ТПУ, 2016. – 42 с.

7. Киселева Т.В., Маслова Е.В. Оптимальное распределение ресурсов при совместном испытании релизов ИТ-сервисов / Технологии разработки информационных систем (ТРИС-201): Сборник трудов VII Международной научно-технической конференции. – Таганрог: Изд. ЮФУ, 2016. – С. 40-44.

8. Киселева Т.В., Маслова Е.В. Применение метода сетевого программирования для решения задач распределения ресурсов при тестировании релизов ИТ-сервисов / Теория активных систем (ТАС-2016): материалы Международной научно-практической конференции. – М.: Изд. ИПУ РАН им. В.А. Трапезникова, 2016. – С. 300-303.

9. Буркова И.В. Метод сетевого программирования в задачах управления проектами: Автореф. дис. докт. техн. наук: 05.13.10. – М.: МГТУ, 2012. – 48 с.

10. Вентцель, Е.С. Теория вероятностей. – М.: Наука, 1969. – 576 с.

References

1. Dotsenko E.Yu., Zhironkina O.V., Agafonov F.V., Genin A.E. Rol' konvergentnyh tehnologij v stanovlenii nepreryvnogo blagopoluchija v neoindu-strial'noj jekonomike [The role of convergent technologies in the development of continuous prosperity in the neoindustrial economy]. Putevoditel' predprinimatelja = Business Guide. 2016. Vol. 32. pp. 65-79.

2. Zhironkin S.A., Zhironkina O.V. Institucional'nye mery strukturnyh preobrazovanij jekonomiki Kemerovskoj oblasti [Institutional Measures of Structural Transformations of the Economy of the Kemerovo Region]. Izvestija Bajkal'skogo gosudarstvennogo universiteta = Letters of Baikal State University. 2013. Vol. 4. pp. 5-10.

3. Nufer L.P, Prokudina M.D. Vnutrennij kontrol' kak faktor bor'by s legalizaciej dohodov, poluchennyh prestupnym putjom [Internal control as a factor in combating the legalization of proceeds from crime]. Sbornik statej mezhdunarodnoj nauchno-prakticheskoj konferencii «Problemy i perspektivy razvitija nauki v Rossii i mire», Ekaterinburg, 2017 = Proceedings of the International scientific and practical conference "Problems and prospects of the development of science in Russia and the world", Ekaterinburg, 2017. Ufa, Aeterna, 2017. pp.: 132-136.

4. Nufer L.P, Prokudina M.D. Protivodejstvie legalizacii dohodov, poluchennyh prestupnym putjom, i vnut-rennij kontrol' v banke [Counteraction to legalization of proceeds from crime and internal control in the bank]. Jekonomika i predprinimatel'stvo = Economics and Entrepreneurship. 2017. Vol. 1(78). pp. 730-734.

5. Kiseleva T.V., Maslova E.V. Analiz informacionnyh riskov / Modelirovanie, programmnoe obespeche-nie i naukoemkie tehnologii v metallurgii: sb. nauch. tr. [Analysis of information risks / Modeling, software and high technology in metallurgy: Procedeeing]. Siberian State Indastrial Unuversity Pub. Novokuzneck. 2011. Pp. 75-80.

6. Zimin V.V. Mehanizmy dekompozicionnogo upravlenija zhiznennym ciklom informacionno-tehnologicheskih servisov (na primere predprijatij chernoj metallurgii) [Mechanisms of decompositional management of the life cycle of information technology services (on example of ferrous metallurgy enterprises)]: Doctoral Thesis: 05.13.01. TPU. Tomsk, 2016. – 42 p.

7. Kiseleva T.V., Maslova E.V. Optimal'noe raspredelenie resursov pri sovmestnom ispytanii relizov IT-servisov / Tehnologii razrabotki informacionnyh sistem (TRIS-201). [Optimal resource allocation in a joint test of IT services releases /]. Proceedings of the VII International Scientific and Technical Conference Information Systems Development Technologies (TRIS-201). South Federal University Pub. Taganrog, 2016. pp. 40-44.

8. Kiseleva T.V., Maslova E.V. Primenenie metoda setevogo programmirovanija dlja reshenija zadach raspredelenija resursov pri testirovanii relizov IT-servisov / Teorija aktivnyh sistem (TAS-2016) [Application of the network programming method for solving resource allocation problems when testing IT service releases]. Proceedings of the International Scientific and Practical Conference Theory of active systems (TAS-2016)]. IPU RAS Pub. Moscow, 2016. – pp. 300-303.

9. Burkova I.V. Metod setevogo programmirovanija v zadachah upravlenija proektami [The method of network programming in project management tasks]: Doctoral Thesis: 05.13.01. MGTU. Moscow, 2012. – 48 p.

10. Ventcel', E.S. Teorija verojatnostej [Probability Theory]. Science. Moscow, 1969. – 576 p.

Авторы

Киселева Тамара Васильевна – доктор технических наук, профессор, кафедра прикладной информатики и программирования, Сибирский государственный индустриальный университет, 654007 Россия, Кемеровская область, Новокузнецк, улица Кирова, 42, e-mail: kis@siu.sibsiu.ru

Маслова Елена Владимировна - аспирант, Сибирский государственный индустриальный университет, 654007 Россия, Кемеровская область, Новокузнецк, улица Кирова, 42.

Authors

Tamara V. Kiseleva – Doctor of Sc., Professor, Department of Applied Informatics and Programming, Siberian State Industrial University, 654007 42 Kirova st., Novokuznezk, Kemerovo region, Russia, e-mail: kis@siu.sibsiu.ru

Elena V. Maslova - post-graduate, Siberian State Industrial University, 654007 42 Kirova st., Novokuznezk, Kemerovo region, Russia

Библиографическое описание статьи

Киселева Т.В. Ресурсный подход к управлению рисками независимого и совместного тестирования релизов IT-сервисов / Т.В. Киселева, Е.В Маслова. // Экономика и управление инновациями. – 2017. – № 2 (2). – С. 33-46.

Reference to article

Kiseleva T.V., Maslova E.V. Resource approach to risk management of independent and joint testing of IT-services releases. Economics And Innovation Management, 2017, no. 2 (2), pp. 33-46. (In Russian).

ISSN 2587-5574