УДК 004.01

МЕТОДИКА КОСВЕННОЙ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ЭЛЕМЕНТОВ МЕТОДОЛОГИИ PRINCE2

Себелев Я.С.

МИРЭА-Российский технологический университет (РТУ МИРЭА), 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: whorespondent@gmail.com

Предложена методика оценки интегральной характеристики ущерба-риска на основе элементов квантификации риска в методологии PRINCE2.

Ключевые слова: методология PRINCE2, резюмирующий профиль рисков, ИТ-проект, безопасность функционирования, риск, реестр рисков.

A TECHNIQUE FOR INDIRECT ASSESSING OF FUNCTIONAL SAFETY IN INFORMATION SYSTEMS USING ELEMENTS OF PRINCE2 METHODOLOGY

Sebelev Y.S.

Federal State Educational Institution of Higher Education "Russian Technological University" (MIREA), 119454, Russia, Moscow, Vernadskogo avenue, 78 e-mail: whorespondent@gmail.com

A method for estimating the integral characteristic of damage-risk based on the elements of risk quantification in the PRINCE2 methodology is proposed.

Key words: PRICE2 methodology, summary risk profile, IT project, safe functioning, risk, risk register.

Введение

В настоящее время идея управления сложными многосоставными объектами неразрывно связана с возникающими в процессе работы рисками, которые подлежат учёту. Подобная ситуация не специфична для сферы ИТ, но возникает во всех сферах деятельности человека, поскольку риск сопряжён с неопределённостью, которая в той или иной степени возникает в любом процессе управления.

В то же время, менеджмент рисков — это камень преткновения современных методологий проектного управления, каждая из которых предлагает свои методики работы с неопределённостью. Всё больше и больше компаний и команд разработчиков переходят на проектное исчисление при создании комплексных информационных продуктов, таких как информационные системы (ИС), чья дороговизна, сложность и величина потенциального воздействия на человека заставляет принимать во внимание возникающие в проекте риски. Одна из таких методологий — PRINCE2 (PRojects IN Controlled Environments) — это британский стандарт управления проектами по созданию информационных систем, который в процессе своего развития стал обобщённым, применимым к любой проектной деятельности.

С другой стороны, управление рисками ИС сопряжено с комплексами программ, которые всегда содержат риски, и их априори невозможно достоверно предсказать и контролировать, но они иногда катастрофически отражаются на качестве функционирования систем или внешней среды. Компании обладают инструментальными средствами управления рисками, которые могут быть недоступны на уровне проекта[2].

Таким образом, управление рисками в ИС сталкивается с необходимостью принимать компромиссные решения, выбирая между эффективностью на уровне предприятия или на уровне проекта[2].

Подходы к управлению риском

На сегодняшний день ряд авторов [1][2][4] предлагают свои подходы к оценке рисков и методы управления ими. Совершенно неудивительно, что отсутствует единое мнение даже относительно определения «риска». Так, согласно ст.2 Федерального закона «О техническом регулировании», риск – это «…вероятность причинения вреда… с учетом тяжести этого вреда». В приложении к опасным производствам, риск аварии рассматривается как мера опасности, характеризующая возможность возникновения аварии и тяжесть ее

последствий[1]. Единым стандартом ISO/IEC 16085 и IEEE 16085-2006 «ИТ. Системная и программная инженерия. Процессы жизненного цикла. Управление рисками» риск определен как вероятность наступления опасного события с его последствиями, а в стандарте ГОСТ РВ 51987-2002 «ИТ. КСАС. Требования и показатели качества функционирования информационных систем. Общие положения» — как возможная опасность неудачи предпринимаемых действий. Здесь риск оценивается с помощью вероятностной меры применительно к анализу и обеспечению безопасности[1]. С другой стороны, риск[2] — негативные события и их величины, отражающие потери, убытки или ущерб от процессов или продуктов, вызванные реализацией угрозы при наличии уязвимости и определенных обстоятельств или событий, приводящих к реализации угрозы при недостатках обоснования, проектирования, разработки и всего жизненного цикла комплексов программ. В данной трактовке риск рассматривается шире, в том числе и как величина, сопряженная элементу проектного исчисления.

В то же время, для программных средств (ПС) и ИС выделяется область анализа и обеспечения — функциональная безопасность[3], связанная с отказовыми ситуациями и потерей работоспособности ИС и ПС вследствие проявления непредумышленных, случайных дефектов и отказов программ, данных, аппаратуры и внешней среды. Наиболее полно степень функциональной защиты системы характеризуется величиной предотвращенного ущерба — риска[3], возможного при проявлении дестабилизирующих факторов и реализации конкретных угроз безопасности применению программного продукта пользователями, а также средним временем между возможными проявлениями угроз, нарушающих безопасность. С этой позиции затраты ресурсов разработчиками и заказчиками на обеспечение безопасности функционирования системы должны быть соизмеримыми с возможным средним ущербом у пользователей от нарушения безопасности. Наиболее общим видом ресурсов, который приходится учитывать при оценке функциональной безопасности, являются допустимые финансово-экономические затраты обеспечения безопасности и средств программной защиты[3]. По приятному совпадению, методологии проектного управления, такие как PRINCE2, включают в себя набор методик и подходов по оценке рисков именно с позиции таких ресурсов. В связи с этим, использование элементов методологии PRINCE2 может содействовать получению интегральной характеристики предотвращенного ущерба-риска.

Управление риском в PRINCE2

Риск в PRINCE2 определяется как неопределённое событие или набор таких событий, в случае реализации которых последует воздействие (позитивное или негативное) на достижение целей проекта. Риск измеряется комбинацией вероятностной характеристики некоторой угрозы и величины её воздействия на цели.[7,8] Угрозы — это всё те же неопределённые события, в случае реализации которых следует негативное влияние на стоящие перед проектом цели. Совокупный эффект рисков на набор целей проекта называется термином подверженности рискам.[7]

Управление риском в методологии PRINCE2 представлено на рис.1 и состоит из четырёх взаимосвязанных шагов и отдельно выделенного «Информирования», поскольку сведения, добытые на каждом шаге, могут послужить причиной для формирования управляющего воздействия до завершения указанного процесса.

Рис. 1. Процесс управления риском в PRINCE2.

Идентификация распадается на две стадии: идентификация контекста и идентификация рисков.

Идентификация контекста предполагает сбор и получение информации о планируемой деятельности, а

также о том, как она вписывается в рынок, общество, организацию. Здесь необходимо представить ответы на вопросы о том, каковы цели проекта, его масштаб, какие предположения были сделаны (например, курс доллара), каковы ограничения данной деятельности и т.д. Здесь используются такие техники, как PESTLE- и SWOT-анализ, изучение перспектив (horizon scanning).

Идентификация риска — процесс распознавания рисков, сопряженных с целями проекта, устроенный таким образом, чтобы минимизировать угрозы. Здесь формируется т.н. реестр рисков, а также формулируются KPI (ключевые показатели эффективности) и EWI (показатели раннего предупреждения). Техники этого этапа: чек-листы, диаграммы Исикавы, метод Делфи и т.д.

Следующий шаг, «Оценка», также декомпозируется на две сущности — индивидуальная и интегральная оценка (не тождественна интегральной характеристике ущерба-риска).

Индивидуальная оценка (рис. 2) заключается в расстановке приоритетов над рисками, чтобы понять, какие из них являются наиболее важными и требующими безотлагательного действия. Для этого необходимо понять, какова вероятность возникновения угрозы, какой количественный эффект они оказывают на достижение цели, а также какова их временная близость.

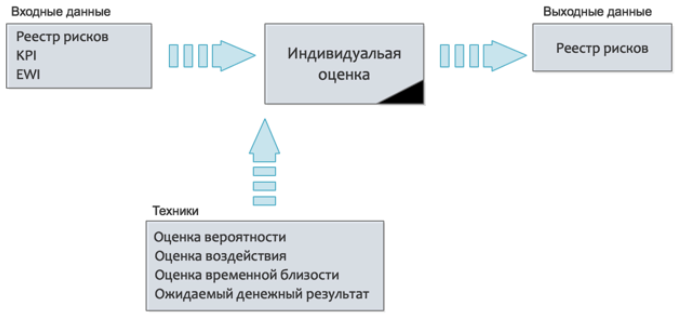

Рис. 2. Определение и информационные потоки индивидуальной оценки риска.

Реестр рисков — это документ, в котором собраны данные по всем идентифицированным угрозам, относящимся к специфической деятельности организации. Формат (таблица, база данных и др.) определяется в каждом случае отдельно, но для каждому риску должен быть присвоен приоритет, стратегия реагирования на риск, а также дата закрытия риска и основания для этого. На данном шаге этот реестр обновляется: в нём появляются вероятностные оценки каждой угрозы, а также оценка их воздействия. Для количественной оценки рисков используются различные техники (рис. 2).

Оценка вероятности записывается в реестр рисков с предварительным условием, что в будущем не будут предприняты никакие действия для изменения этой вероятности.

Оценка временной близости основывается на том, что риски изменчивы во времени и не бывают постоянными. Она показывает срочность необходимой реакции на риск, распределение во времени и необходимые триггеры этой реакции.

Ожидаемый денежный результат (ОДР) высчитывается умножением оценки воздействия индивидуального риска на его вероятность, выдавая, таким образом, для каждого риска его весовой денежный коэффициент. ОДР каждого риска представляет собой квантификацию подверженности проекта этому риску, однако сам по себе ОДР даёт мало информации, поскольку в случае реализации риска взыскивается вся величина из оценки воздействия, а не ОДР, где учитывается вероятность. Тем не менее, совокупная величина ОДР для всех рисков для данной деятельности позволяет увидеть подверженность риску для данного вида деятельности, выраженную в денежных единицах. Для ОДР рекомендуется создавать трёхточечную оценку (наилучший, наихудший и наиболее вероятный вариант). Кроме того, может быть введен полный ожидаемый денежный результат (ПОДР) для конкретной деятельности. Он вычисляется агрегированием ОДР с учётом связи рисков между собой (взаимоисключение-дополнение).

Интегральная оценка (рис. 3) позволяет высчитать подверженность риску для некоторой деятельности в виде совокупного эффекта идентифицированных в реестре рисков угроз.

Следующий шаг в управлении рисками — «планирование». Здесь представлены конкретные специфические ответные реакции на возникающие идентифицированные угрозы. На этом шаге большой упор делается на обеспечение отсутствия возникновения эффекта неожиданности от реализации какого-либо риска из ранее описанных в реестрах. Методика анализа результативности затрат и дерево решений широко используются на стадии планирования.

Рис. 3. Определение и информационные потоки интегральной оценки риска.

Наконец, шаг «реализация» — последний в процедуре управления риском. Цель данного этапа — обеспечение внедрения и использования распланированных действий по управлению риском, их мониторинг по эффективности, а также принятие управленческих корректирующих действий, если ответные реакции из стадии «планирования» не приносят удовлетворительных результатов. Поскольку в структуре своей процесс управления рисками — итеративный, то и на реализации всё не заканчивается, и получаемая новая информация служит субстратом для обновления суммарного профиля рисков и выработки оценки тенденции подверженности риску.

Резюмирующий профиль рисков ИТ-проекта

Согласно [4] под БФИС понимается свойство ИС противодействовать появлению аварийных ситуаций, влияющих отрицательно на жизнедеятельность человека и окружающую среду, при функционировании ИС в соответствии с целевым назначением. В терминологии PRINCE2 аварийные ситуации обозначаются зонтичным термином «исключение». В контексте БФИС рассматривается исключение по риску, которое, будучи возвращено, означает переход элемента(-ов) ИС в критический процесс[7]. Таким образом, задача управления риском наиболее четко отражена в выработке и реализации управляющих корректирующих действий (шаг «планирование») и, что наиболее важно, недопущении реализации наиболее опасных рисков («индивидуальная и интегральная оценка»). Последнее может быть представлено в виде резюмирующего профиля рисков. Пример такого профиля для проекта по переносу данных между репозиториями на основе [6] представлен на рис. 4.

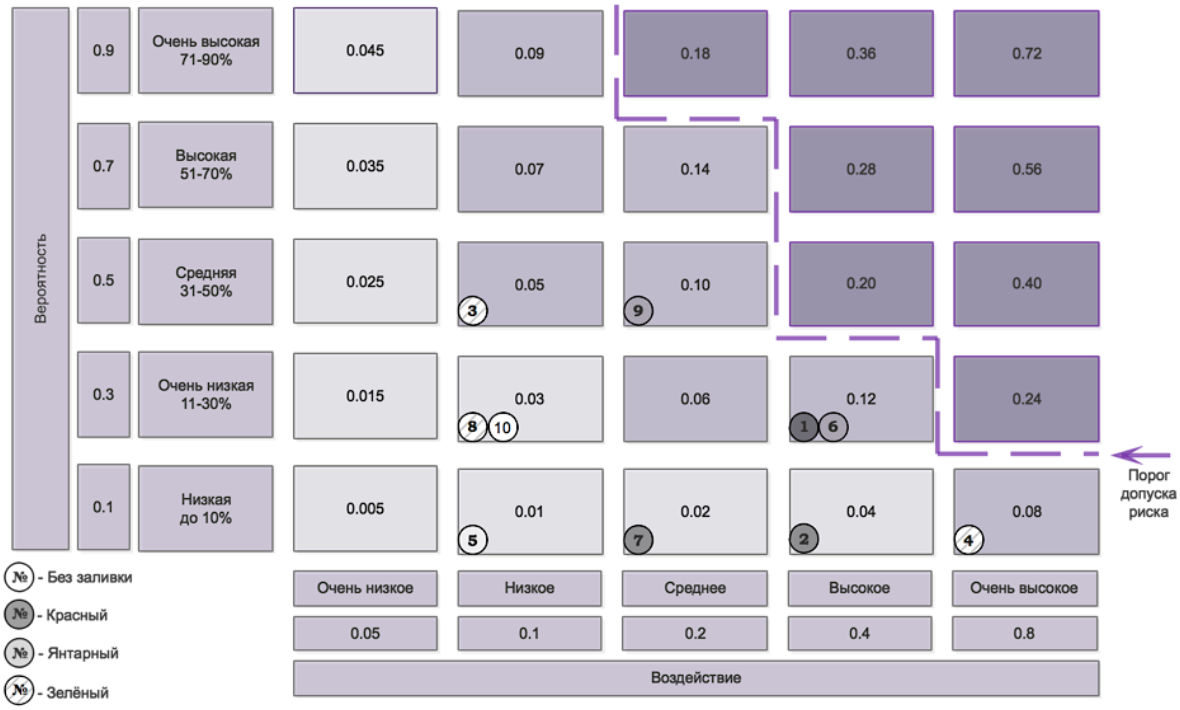

Рис. 4. Резюмирующий профиль рисков проекта.

В резюмированном профиле рисков были установлены 10 наиболее существенных рисков, ассоциированных с процессом миграции данных между репозиториями посредством SAAS-средств[6]:

1. Раскрытие конфиденциальной информации клиентов;
2. Нарушение целостности данных;
3. Ошибки при подготовке данных в исходном репозитории;
4. Несовместимость исходной архитектуры с конечной;
5. Отказ SAAS-сервиса;
6. Правовые коллизии (договор об ответственном хранении данных);
7. Задержка переделегирования на новые DNS-серверы;
8. Сбой/отказ на существующем хранилище;
9. Угрозы безопасности, ассоциированные с миграцией;
10. Неверная конфигурация сайта на новом хранилище.

Под воздействием в данном случае понимается весовой коэффициент времени, на которое придётся отложить запуск сайта в эксплуатацию, иными словами, дополнительное время, в течение которого сайт не будет доступен конечному пользователю. Для удобства эту характеристику нормируют в пределах единицы.

Таблица 1. Определение шкалы воздействий.

Воздействие	Время	Предпринимаемые действия
Очень высокое	>11 дней	Закрытие проекта с исключением
Высокое	8-10 дней	Изменение бизнес-причины проекта
Среднее	4-7 дней	Обновление динамического плана
Низкое	1-2 дня	Создание исключения
Очень низкое	<1 дня	Небольшие уступки пользователям

Кроме того, в профиле представлен так называемый порог допуска риска, отмеченный прерывистой линией на рис. 4. Он показывает общий уровень риска, который организация готова допустить в данной ситуации. Также на рис. 4 используется идентификация отдельных рисков в нотации RAG (Red Amber Green, Красный, Янтарный, Зелёный) с тем, чтобы не просто указать риск в системе координат «Вероятность - Воздействие», но и показать статус работы над этим риском.

Таблица 2. Статус риска в нотации RAG.

Цвет	Статус
Нет цвета	Прогресс нельзя измерить, поскольку действие над риском невозможно до определённой даты
Красный	Работа над риском безрезультатна
Янтарный	Средний прогресс в управлении риском с немногочисленными данными о результатах такого управления
Зелёный	Управление риском происходит в данный момент, согласовано со стадией проекта, с достаточными данными о результатах

Предотвращенный ущерб-риск и PRINCE2

В качестве оценки величины предотвращенного ущерба-риска для ИС веб-сайта в момент переноса данных между двумя репозиториями посредством SAAS-средств предлагается воспользоваться методикой оценки ПОДР из PRINCE2. Согласно [5], день простоя небольшого Интернет-магазина с годовым доходом 400.000 ₽ и 10-ю сотрудниками стоит около 30.000 ₽ (продажи и производительность труда). На основании резюмированного профиля рисков получаем оценку ОДР (Таблица 3).

Для вычисления ПОДР требуется проверить указанные риски на корреляцию. Например, сбой/отказ на существующем хранилище (№8) обозначает реализацию риска №3 — ошибки при подготовке данных в исходном репозитории и т.д. (Таблица 3). При двусторонней корреляции выбирается больший ОДР, при односторонней — ОДР суммируется[7]. Кроме того, реализация рисков №4 и №6 приводит к остановке деятельности сайта, что означает простой по ожидаемому количеству дней без учёта вероятностного коэффициента, а также делает бессмысленным учёт остальных рисков. Получаемая таким образом величина — ОДР, нормализованная по корреляции.

Таблица 3. Оценка ожидаемого денежного результата реализации рисков.

№ риска	Вероятность, %	Воздействие, дней	Коррелят, № риска	ОДР, рублей	ОДРкорр
1	30	9	9	81.000	81.000
2	10	9	9	27.000	81.000
3	50	1.5	-	22.500	22.500
4	10	11	!	33.000	363.000
5	10	1.5	-	4500	4500
6	30	9	!	81.000	729.000
7	10	5	-	15.000	15.000
8	30	1.5	3	13.500	36.000
9	50	5	1, 2	75.000	81.000
10	30	1.5	-	13.500	13.500
			ИТОГО:	ПОДР	334.500
				ПОДР(№3)	363.000
				ПОДР(№6)	729.000

Таким образом, на выходе получено три значения ПОДР, которые показывают подверженность риску по нотации PRINCE2, и которые одновременно можно представлять как величины предотвращенного ущерба-риска при оценке функциональной безопасности ИС веб-сайт в момент миграции данных между двумя репозиториями посредством SAAS-средств.

Заключение

Предложен метод косвенной оценки функциональной безопасности ИС сайта в момент миграции данных между двумя репозиториями с использованием SAAS-средств на основе величины предотвращенного ущерба-риска. В свою очередь, оценка данной величины произведена на основе методики подсчёта полного ожидаемого денежного результата из методологии PRINCE2. Полученные значения, будучи сравнены с годовой выручкой предприятия, позволяют говорить о низкой функциональной безопасности описываемого решения.

Список литературы

1. Костогрызов А.И. Прогнозирование рисков для обеспечения эффективности систем информационной безопасности в их жизненном цикле. Правовая информатика, 2013.
2. Липаев В.В. Анализ и сокращение рисков проектов сложных программных средств. - М.: СИНТЕГ, 2005. - 224 с. (Серия «Управление качеством»).
3. Липаев В.В. Программная инженерия. Методологические основы. Москва, 2006.
4. Петров А.Б. Методы и алгоритмы анализа элементов устройств вычислительной техники и систем управления на предсказуемость поведения — Москва, 2005.
5. Расчёт стоимости простоя. Режим доступа: http://www.fnc-group.ru/en/business-impact-analysis.htm [Электронный ресурс]
6. Себелев Я.С. Опыт применения методологии PRINCE2 для ИТ-проекта миграции данных между репозиториями. ИТ-Стандарт, 2017,
Т.1. № 3-1 (12).
7. Management of Risk: Guidance for Practitioners. // Crown Copyright — 2010. Third edition. ISBN: 9780113312740
8. Managing Successful Projects with PRINCE2. // Copyright AXELOS Limited 2017 — Sixth edition. ISBN: 9780113315338.

References

1. Kostogrizov A.I. Risk prediction for ensuring efficacy of information security systems in its lifecycle, 2013.
2. Lipaev V.V. B.B. Analysis and risk reduction in IT-projects of complex software, 2005.
3. Lipaev V.V. Software engineering. Methodological framework, 2006.
4. Petrov A.B. Methods and algorithms of predictability analysis in elements of computing machinery and control

systems — Moscow, 2005
5 Business impact analysis. Link: http://www.fnc-group.ru/en/business-impact-analysis.htm
6. Sebelev Y.S. An application of PRINCE2 methodology to an IT project of data migration between repositories. IT-Standard, 2017.
7. Management of Risk: Guidance for Practitioners. // Crown Copyright — 2010. Third edition. ISBN: 9780113312740
8. Managing Successful Projects with PRINCE2. // Copyright AXELOS Limited 2017 — Sixth edition. ISBN: 9780113315338.