

DOI: 10.21821/2309-5180-2023-15-6-1105-1114

RISK MANAGEMENT IN SOFTWARE DEVELOPMENT IN THE FIELD OF INFORMATION PROTECTION

I. M. Yastrebov

YADRO SOFTWARE DEVELOPMENT CENTER, LLC., Moscow, Russian Federation

In the context of increasing digitalization of sea and river transport, the immersion of the entire transport infrastructure in the digital environment, the volume of information flows serving the transport process is increasing, and the requirements for information protection are increasing in conditions of an aggressive external information environment. In the digital environment, a software product must not only serve the document flow of transport chains, but also ensure its confidentiality. Automation of transport facilities (ships, platforms, berths, warehouses) management increases their potential vulnerability from unauthorized access to control systems; the latter must be taken into account in servicing programs, increasing their size (for example, there is a need to fragment coherent information blocks and their alternative routing). This, in turn, increases the risk of errors in the software products themselves and significantly complicates their structure. Risks of failures (including confidentiality violations) during the software operation that implements information exchange can entail significant material and reputational losses for the developer. If the developer is legally and functionally involved in the industry, such losses can and should be considered among the general range of risks in water transport. An important aspect of risk management, which until recently was practically not considered in a quantitative aspect within the framework of mathematical models, is the joint consideration of losses when a risk situation occurs and the developer's costs associated with reducing the likelihood of such occurrences; the latter may entail a reduction in the total expected losses, formalized as the corresponding mathematical expectation. As a result, risk management can be formulated in terms of mathematical programming problems with different (discrete or continuous) sets of constraints and with different properties of objective functions.

Keywords: risk management, optimizing, math modeling, information flows, software development, program complexity.

For citation:

Yastrebov, Ivan M. "Risk management in software development in the field of information protection." *Vestnik Gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S. O. Makarova* 15.6 (2023): 1105–1114. DOI: 10.21821/2309-5180-2023-15-6-1105-1114.

УДК 004.6:656.6

УПРАВЛЕНИЕ РИСКАМИ ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

И. М. Ястребов

ООО «ЯДРО ЦЕНТР ПРОГРАММНЫХ РАЗРАБОТОК», Москва, Российская Федерация

Темой работы является исследование проблем, связанных с возрастающим объемом обслуживающих транспортный процесс информационных потоков и повышением требований к защите информации в условиях агрессивной внешней информационной среды в условиях нарастания цифровизации морского и речного транспорта, а также трансформации в ней всей транспортной инфраструктуры. В цифровой среде программный продукт должен не только обслуживать документооборот транспортных цепочек, но и обеспечивать его конфиденциальность. Автоматизация управления транспортными объектами (суда, платформы, причалы, склады) увеличивает их потенциальную уязвимость от несанкционированного доступа к системам управления; последнее должно учитываться в обслуживающих программах, увеличивая их размер (например, возникает необходимость дробления связанных информационных блоков и их альтернативной маршрутизации). Это в свою очередь повышает риски появления ошибок в самих программных продуктах, и значительно усложняет их структуру. Риски сбоев (в том числе нарушения конфиденциальности) при работе программного обеспечения, реализующего информационный обмен, могут повлечь за собой для разработчика существенные материальные и репутационные потери. В случае юридической и функциональной включенности разработчика в отрасль такие потери могут и должны рассматриваться в общем ряду

рисков на водном транспорте. Важным аспектом управления рисками, который до последнего времени практически не рассматривался в количественном аспекте в рамках математических моделей, является совместное рассмотрение потерь при наступлении ситуации риска и затрат разработчика, связанных с уменьшением вероятностей таких наступлений; последнее может повлечь уменьшение общих ожидаемых потерь, формализованных как соответствующие математические ожидания. В результате управление рисками может быть сформулировано в терминах задач математического программирования с различными (дискретными либо непрерывными) множествами ограничений и различными свойствами целевых функций.

Ключевые слова: управление рисками, оптимизация, математическое моделирование, информационные потоки, программирование, сложность программ.

Для цитирования:

Ястребов И. М. Управление рисками при разработке программного обеспечения в области защиты информации / И. М. Ястребов // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2023. — Т. 15. — № 6. — С. 1105–1114. DOI: 10.21821/2309-5180-2023-15-6-1105-1114.

Введение (Introduction)

Общие положения национального стандарта по управлению рисками¹ требуют в случае проектов по созданию программного обеспечения (ПО) дальнейшей конкретизации. В источнике [1, с. 28] отмечается следующее: «Руководители проектов часто уверяют, что клиенты никогда не пойдут ни на один проект, если будут понимать риски». Тем не менее, по мнению самих руководителей, такое понимание, безусловно, необходимо при календарном планировании проекта и распределении человеческих (прежде всего) ресурсов. В [2, с. 24] количественное (в отличие от многих качественных, описательных) определение риска как математическое ожидание случайной величины ущерба служит отправной точкой для дальнейшей детализации и перехода от оценки вероятностей наступления рисков к минимизации связанных с этим вероятных потерь.

Риск-факторы по своей природе являются случайными, поэтому управление рисками в количественных аспектах должно основываться на теоретико-вероятностной методологии [3]. Важной и неизбежной отправной точкой является определение исходных вероятностей и распределений для параметров, включаемых в математическую модель. Здесь наряду с экспертными априорными оценками (в том числе байесовский подход, когда определение вероятности как относительной частоты дополняется ее субъективной оценкой) может привлекаться аппарат регрессионного анализа.

Анализ публикаций в периодических изданиях и электронных публикаций по проблеме управления рисками при разработке ПО (например, [4]–[6] и др.) показывает, что практически во всех случаях речь идет лишь о содержательном перечислении некоторых неблагоприятных ситуаций, без построения каких-либо математических моделей, выводящих риск-менеджмент при разработке ПО на количественные критерии. Отчасти такое положение дел связано с тем, что некоторые и, возможно, важные факторы риска трудно поддаются количественной оценке и упреждению. В этой связи необходимо отметить наиболее важные из них [7]:

- изменение состава команды разработчиков в ходе исполнения проекта;
- неправильная оценка компетенций членов команды разработчиков;
- изменения требований заказчика к функционалу программного продукта;
- излишний оптимизм при назначении сроков;
- отсутствие навыков проектного менеджмента, хищение исходного кода, нарушение закона об авторском праве [8] и т. п.

Предлагаемые в этих публикациях упреждающие мероприятия, такие, например, как «правильная организация процесса», «процесс разработки должен быть гибким», правильные по своей сути, вряд ли можно безоговорочно включить в какую-либо математическую модель риск-менеджмента. В то же время некоторые IT-разработки на водном транспорте (возможно, впервые для решения данной проблемы) были ориентированы на создание теоретико-вероятностных математических моделей (в том числе оптимизационных [9]–[11]), объединяющих вероятности одновременных

¹ ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. М.: Стандартинформ, 2020. 14 с.

и разновременных, единичных и каскадных рисков с потерями при их наступлении и затратами на снижение указанных вероятностей [9]–[15].

Методы и материалы (Methods and Materials)

В соответствии с исследуемой концепцией исходной предпосылкой для математического моделирования риск-менеджмента при разработке защитного ПО будем считать следующее предположение: за счет увеличения материальных затрат и рабочего времени можно снизить до некоторого уровня вероятность p наступления любого риск-фактора, а значит, и математическое ожидание сопутствующих потерь, но при этом существует вероятность того, что дополнительные расходы могут превысить ожидаемые потери при больших значениях p . Это предопределяет многовариантность задачи и необходимость привлечения методов математического программирования

Разработка программного обеспечения в области защиты информации, как правило, реализуется в рамках больших проектов, в которых участвуют несколько подразделений компании-разработчика. Риски ошибок возникают при этом как внутри отдельного подразделения (группы разработчиков отдельного программного модуля), так и на стадии их сопряжения в более крупные блоки.

Процесс разработки большого ПО является стадийным. Представляется, что количественные методы риск-менеджмента по своей природе применимы прежде всего к следующим стадиям:

- создание исходного кода;
- внутреннее тестирование;
- мониторинг базового периода эксплуатации.

К риск-факторам, учитываемым в рамках предлагаемой модели, относятся:

- превышение сроков разработки программного продукта в целом либо его отдельных модулей;
- ошибки программирования.

За рамками модели, таким образом, остаются внешние риск-факторы — такие, как, например, изменение требований заказчика, изменение законодательства, внеэкономическое изменение структуры рынка и его условий (санкции), волатильность валютного рынка и др.

В процессе исследования были использованы следующие инструменты снижения рисков.

1. *Оценка влияния сложности программ на затратную оценку риска.* Известен неформальный подход к определению сложности программного продукта (обозначим этот параметр через s), действующий, разумеется, «в среднем», когда уровень сложности программного продукта (ПП) напрямую связан с его длиной l . Априори здесь естественно предполагать прежде всего линейную либо квадратичную зависимость. Будем считать программный модуль сложным (и, значит, подверженным специфическим рискам, связанным с программированием) в следующих случаях:

1. Если число M функционально-тематически ориентированных групп разработчиков подмодулей не менее порогового значения M_0 (в частности, в предельном случае отдельная группа может состоять из одного разработчика); разумеется, неравенство для M_0 может назначаться в каждом случае исходя из индивидуальных особенностей проекта.

2. Если код имеет большой прогнозный размер l (без учета возможности реализации риск-факторов). Следует отметить, что l — труднопрогнозируемый параметр. Возможна его экспертная оценка с привлечением моделей нечеткой логики и нечетких множеств [16]. Другой широко используемой является оценка по количеству функциональных точек (FPA), регламентированная в ISO 20296:2009. Данная методика измерения программного продукта базируется на фиксации и подсчете единиц пользовательского функционала. Указанным стандартом задаются исходные дефиниции и описывается алгоритм метода измерения функциональных размеров (FSM) [17];

В качестве апостериорной альтернативы, в отличие от априорной (экспертной), укажем на оценку в тысячах строк ([klc] — kilo lines of code). Анализ литературы показывает, что в последнем случае в примерах для сложных программ нижняя граница для l составляет 20 klc. Представляется важным следующее методологическое замечание: *если каким-либо путем может быть получена интегральная количественная оценка R риска проекта (либо его отдельного этапа) как безразмерная*

вероятность или размерная (затратная), то интерес представляет прежде всего не абсолютное значение R , которое само по себе малоинформативно, а сравнение значений R , рассчитанных по единой методике для альтернативных способов построения логической, кадровой и календарной структуры всего проекта.

3. Современные технологии программирования предусматривают поступление набора разработанных подмодулей для сопряжения (сборки, настройки и тестирования — development & operations) отдельному исполнителю (dev-ops-инженеру). При этом одной из его функций является security-engineering, включающая разработку и запуск тестов, анализирующих возможные уязвимости. Вероятность их появления повышается именно при сопряжении частей кода, выполненных разными разработчиками. Последнее означает, что логическая структура исполнения ПП может быть представлена ориентированным графом.

4. Для каждого исполнителя исходным календарным планом — сетевым графиком при его графическом представлении — задано время исполнения t . С учетом современных технологий разработки программного продукта рассмотрим ситуацию с N разработчиками отдельных программных модулей ($PK_1, PK_2, \dots, PK_N$) и dev-ops-инженером (PK_0).

II. Математическая модель минимизации рисков потерь. С каждым разработчиком $j = 0, 1, \dots, N$ свяжем набор параметров, задающих сигнатуру модуля, т. е. количественные плановые значения (l_j, t_j) . Далее для каждого j введем следующие параметры:

— зависимость вероятности p_j наступления превышения Δt плановой длительности от этого превышения:

$$p_j = p_j(\Delta t);$$

— зависимость вероятных потерь $\Delta^t z_j$ от превышения Δt :

$$\Delta^t z_j = \Delta^t z_j(\Delta t);$$

— зависимость вероятности π_j наступления превышения Δl планового размера ПП от этого превышения:

$$\pi_j = \pi_j(\Delta l);$$

— зависимость вероятных потерь $\Delta^l z_j$ от превышения Δl :

$$\Delta^l z_j = \Delta^l z_j(\Delta l)$$

(заметим, что если размер ПП измеряется количеством функциональных точек, то через параметр Δl находит свое выражение риск изменения требований заказчика уже в ходе создания ПП).

Естественно предполагать, что функции p_j и π_j должны иметь убывающий характер, а функции $\Delta^t z_j, \Delta^l z_j$ — возрастающий.

Рассмотрим сначала дискретную постановку. Будем в этом случае исходить для j -го исполнителя из набора реперных точек превышения по времени:

$$\Delta t_1 < \Delta t_2 < \dots < \Delta t_n$$

и аналогичного набора превышений изначально предполагаемого размера ПП:

$$\Delta l_1 < \Delta l_2 < \dots < \Delta l_m.$$

На основе ранее использованных обозначений введем:

$\Delta^t z_{ji}$ — рискованные потери при реализации рискованного фактора Δt_i для j -го исполнителя;

$\Delta^l z_{ji}$ — рискованные потери при реализации рискованного фактора Δl_i для j -го исполнителя.

В этом случае функции p_j и π_j реализуются наборами констант — соответственно $p_{ji} = p_j(\Delta t_i)$, $\pi_{ji} = \pi_j(\Delta l_i)$. Назначение (экспертное) вероятностей должно обеспечивать свойство законов распределения:

$$\sum_{i=1}^n p_{ji} = 1; \quad \sum_{i=1}^m \pi_{ji} = 1; \quad j = 1, \dots, N.$$

Если изначально в усредненных экспертных оценках это равенство не выполняется (что естественно, поскольку оценки разных экспертов независимы), следует перейти от них к средневзвешенным величинам:

$$p_{jk} := p_{jk} / \sum_{i=1}^n p_{ji}; \quad \pi_{jk} := \pi_{jk} / \sum_{i=1}^m \pi_{ji}; \quad j = 0, 1, \dots, N. \quad (1)$$

Реализация рисков Δt_{ji} , Δl_{ji} предполагает, что «по пути» были реализованы риски с меньшими значениями $\Delta t_{j1}, \dots, \Delta t_{j,i-1}$ и $\Delta l_{j1}, \dots, \Delta l_{j,i-1}$; это должно находить отражение в задании затратных функций что, однако, не означает обязательный равномерный рост (линейность). Тогда вероятные дополнительные рисковые затраты $\Delta z_{\text{риск}}^{\text{пасс}}$ для отдельного j -го исполнителя группы разработчиков задаются выражениями (математическими ожиданиями) случайной величины $\Delta Z_j^{(t)}$, имеющей закон распределения $(\Delta^t z_{j1}, \dots, \Delta^t z_{jn}; p_{j1}, \dots, p_{jn})$, и случайной величины $\Delta Z_j^{(l)}$, имеющей закон распределения $(\Delta^l z_{j1}, \dots, \Delta^l z_{jm}; \pi_{j1}, \dots, \pi_{jm})$. Суммирование этих затрат по всем исполнителям дает формулу

$$\Delta z_{\text{риск}}^{\text{пассив}} = \sum_{j=0}^N \left(\sum_{i=1}^n p_{ji} \Delta^t z_{ji} + \sum_{i=1}^m \pi_{ji} \Delta^l z_{ji} \right). \quad (2)$$

Если на стадии планирования разработки программного продукта сразу добавить $\Delta z_{\text{риск}}^{\text{пасс}}$ к базовой стоимости разработки, то такой — *пассивный* — риск-менеджмент означает фактический отказ от управления рисками (хотя остается актуальной задача адекватного назначения функций p_j и π_j , а также функций затрат $\Delta^t z_j$, $\Delta^l z_j$). В противоположность этому управление рисками с помощью математического моделирования в описываемой далее постановке исходит из предполагаемой возможности уменьшения риск-факторов Δt и Δl за счет дополнительных *упреждающих*, (*профилактических*) затрат, что может оказаться выгодным, если итоговые вероятные затраты на выполнение проекта уменьшатся.

Итак, математическая модель управления рисками при создании ПП может быть формализована путем совместного рассмотрения двух разнонаправленных тенденций: уменьшение математического ожидания дополнительных потерь при уменьшении вероятностей p_j , π_j , но при этом одновременное возникновение дополнительных затрат для обеспечения этих новых значений вероятностей (например, при увеличении числа разработчиков, либо за счет сверхурочной работы коллектива и т. д.).

Введем (для простоты одинаковые для каждого j -го исполнителя) функции Δp_i , $\Delta \pi_i$, $0 \leq \Delta p_i \leq 1$, $i = 1, \dots, n$, $0 \leq \Delta \pi_i \leq 1$, $i = 1, \dots, m$, связанные с целенаправленным уменьшением вероятностей p_{ji} , π_{ji} до значений $\tilde{p}_{ji}$, $\tilde{\pi}_{ji}$ следующим образом:

$$\tilde{p}_{ji} = p_{ji}(1 - \Delta p_i), \quad \tilde{\pi}_{ji} = \pi_{ji}(1 - \Delta \pi_i).$$

Предположим, что эти новые вероятности сохраняют свойство монотонного убывания по i . При этом, однако, $\sum_{i=1}^n \tilde{p}_{ji} < 1$, $\sum_{i=1}^m \tilde{\pi}_{ji} < 1$. Возникающие невязки устраняются при расширенном истолковании распределений случайных величин $\Delta Z_j^{(t)}$ и $\Delta Z_j^{(l)}$. Именно отсутствующие при пассивном управлении затраты $\Delta u_{j1}, \dots, \Delta u_{jn}$ и $\Delta v_{j1}, \dots, \Delta v_{jm}$ на уменьшение значений p_{ji} , π_{ji} понимаются как имеющие нулевые вероятности, т. е. законы распределения записываются в виде:

$$(\Delta^t z_{j1}, \dots, \Delta^t z_{jn}, \Delta u_{j1}, \dots, \Delta u_{jn}; p_{j1}, \dots, p_{jn}, 0, \dots, 0); (\Delta^l z_{j1}, \dots, \Delta^l z_{jm}, \Delta v_{j1}, \dots, \Delta v_{jm}; \pi_{j1}, \dots, \pi_{jm}, 0, \dots, 0),$$

а при активном управлении эти законы приобретают для уже ненулевых дополнительных затрат ненулевые вероятности:

$$(\Delta^t z_{j1}, \dots, \Delta^t z_{jn}, \Delta u_{j1}, \dots, \Delta u_{jn}; p_{j1}(1 - \Delta p_1), \dots, p_{jn}(1 - \Delta p_n), p_{j1}\Delta p_1, \dots, p_{jn}\Delta p_n)$$

и, соответственно,

$$(\Delta^l z_{j1}, \dots, \Delta^l z_{jm}, \Delta v_{j1}, \dots, \Delta v_{jm}; \pi_{j1}(1 - \Delta \pi_1), \dots, \pi_{jm}(1 - \Delta \pi_m), \pi_{j1}\Delta \pi_1, \dots, \pi_{jm}\Delta \pi_m).$$

В этом случае выполняется необходимое равенство для сумм вероятностей.

В результате ожидаемые потери при активном управлении рисками задаются меньшим значением

$$\Delta z_{\text{риск}}^{\text{актив}} = \sum_{j=0}^N \sum_{i=1}^n p_{ji} (1 - \Delta p_i) \Delta^t z_{ji} + \sum_{j=0}^N \sum_{i=1}^m \pi_{ji} (1 - \Delta \pi_i) \Delta^l z_{ji}, \quad (3)$$

а дополнительные затраты $Z_{\text{риск}}^{\text{актив}}$ имеют вид

$$Z_{\text{риск}}^{\text{актив}} = \sum_{j=0}^N \sum_{i=1}^n p_{ji} \Delta p_i \Delta u_{ji} + \sum_{j=0}^N \sum_{i=1}^m \pi_{ji} \Delta \pi_i \Delta v_{ji} = \sum_{i=1}^n \Delta p_i \sum_{j=0}^N p_{ji} \Delta u_{ji} + \sum_{i=1}^m \Delta \pi_i \sum_{j=0}^N \pi_{ji} \Delta v_{ji}. \quad (4)$$

$$\text{Обозначим } \Delta \tilde{u}_i = \sum_{j=0}^N p_{ji} \Delta u_{ji}, \quad \Delta \tilde{v}_i = \sum_{j=0}^N \pi_{ji} \Delta v_{ji}.$$

Тогда $Z_{\text{риск}}^{\text{актив}} = \sum_{i=1}^n \Delta p_i \Delta \tilde{u}_i + \sum_{i=1}^m \Delta \pi_i \Delta \tilde{v}_i$ линейно зависит от Δp_i и $\Delta \pi_i$. Тем не менее результирующий эффект активного управления:

$$\Theta_{\text{риск}}^{\text{актив}} = \Delta z_{\text{риск}}^{\text{пасс}} - \Delta z_{\text{риск}}^{\text{актив}} - Z_{\text{риск}}^{\text{актив}}, \quad (5)$$

нельзя включить в задачу линейного программирования в качестве максимизируемой целевой функции ввиду того, что условия на допустимые значения управляемых переменных Δp_i и $\Delta \pi_i$, связанные с обеспечением монотонности вероятностей, не гарантируют невыпуклость множества ограничений на управляемые переменные.

Перебор различных стратегий управления, связанных с изменениями настраиваемых параметров модели (2)–(4) позволяет риск-менеджменту выбрать вариант, соответствующий максимальному положительному эффекту. Формулы (2) существенно упрощаются, если риск-менеджмент ограничится для каждого j единственным возможным значением для превышения времени исполнения и превышения размера кода: Δt , Δl и, соответственно, параметрами Δp , $\Delta \pi$. Для этого случая запишем:

$$\Delta z_{\text{риск}}^{\text{актив}} + Z_{\text{риск}}^{\text{актив}} = \sum_{j=0}^N p_j (1 - \Delta p) \Delta^t z_j + \pi_j (1 - \Delta \pi) \Delta^l z_j + \Delta p \cdot p_j \Delta u_j + \Delta \pi \cdot \pi_j \Delta v_j.$$

В данном случае (в соответствии с известным в математической статистике компромиссом «точность vs надежность») уменьшение количества необходимых экспертных оценок повышает надежность модели. Возможно, на практике управление рисками будет исходить (в том числе из-за взаимозависимости параметров) из априорно заданного приемлемого значения $Z_{\text{риск}}^{\text{актив}}$, которое управление проектом готово принять. Тогда должно быть рассчитано новое значение рискованных потерь, для чего нужно пересчитать вероятности превышений. Для этого находятся значения $i = i_t$, $i = i_l$, для которых нарастающие суммы рискованных потерь:

$$\Delta_{i_t} z_{\text{риск}}^{\text{актив}} = \sum_{j=0}^N \sum_{i=1}^{i_t} p_{ji} (1 - \Delta p_i) \Delta^t z_{ji} + \sum_{j=0}^N \sum_{i=1}^{i_l} \pi_{ji} (1 - \Delta \pi_i) \Delta^l z_{ji}, \quad (6)$$

оказываются наиболее близкими снизу к упреждающим затратам $Z_{\text{риск}}^{\text{актив}}$. Тогда полный результат активного управления с учетом потерь и затрат

$$P_{\text{риск}}^{\text{актив}} = \sum_{j=0}^N \sum_{i=i_t+1}^n \Delta p_i p_{ji} \Delta u_{ji} + \sum_{j=0}^N \sum_{i=i_l+1}^m \Delta \pi_i \pi_{ji} \Delta v_{ji} + Z_{\text{риск}}^{\text{актив}}, \quad (7)$$

а эффект

$$\Theta_{\text{риск}}^{\text{актив}} = \Delta z_{\text{риск}}^{\text{пассив}} - P_{\text{риск}}^{\text{актив}}. \quad (8)$$

В континуальной постановке вероятность $p_j(\Delta t)$ превышения планового срока на Δt для j -го исполнителя рассматривается как непрерывная функция от Δt и служит плотностью распределения случайной величины — функции вероятных рискованных потерь $\Delta^t z_j(\Delta t)$; аналогичный смысл имеют, соответственно, функции $\pi_j(\Delta l)$ и $\Delta^l z_j(\Delta l)$. Пусть ΔT , ΔL — реальные границы

возможного изменения параметров Δt , Δl (аналоги Δt_n , Δl_m дискретного случая). Среднее значение пассивных (в прежнем смысле) рискованных потерь представляется интегральным выражением

$$\Delta_j z = \int_0^{\Delta T} p_j(\Delta t) \Delta' z_j(\Delta t) d(\Delta t) + \int_0^{\Delta L} \pi_j(\Delta l) \Delta' z_j(\Delta l) d(\Delta l),$$

а полные рискованные потери

$$\Delta z_{\text{риск}}^{\text{пассив}} = \sum_{j=0}^N \Delta_j z.$$

С целью математического моделирования активного риск-менеджмента введем по аналогии с дискретным случаем экспертным путем для каждого j функцию $\Delta p(\Delta t)$, отвечающую следующим ограничениям:

- $p_j(\Delta t)$ не возрастает;
- $p_j(\Delta t)(1 - \Delta p(\Delta t))$ не возрастает;
- $0 \leq \Delta p(\Delta t) \leq 1$.

Далее вновь следует рассмотреть следующие затраты:

- $\Delta u(\Delta t)$ на снижение пассивно ожидаемой вероятности $p_j(\Delta t)(1 - \Delta p(\Delta t))$ до величины $p_j(1 - \Delta p_j)$
- $\Delta v(\Delta l)$ на мероприятия по снижению пассивно ожидаемой вероятности $\pi_j(\Delta l)$ на величину $\pi_j(\Delta l)(1 - \Delta \pi(\Delta l))$.

Обозначим $\tilde{p}_j(\Delta t) = p_j(\Delta t)(1 - \Delta p(\Delta t))$, $\tilde{\pi}_j(\Delta l) = \pi_j(\Delta l)(1 - \Delta \pi(\Delta l))$. Тогда ожидаемые рискованные затраты при активном менеджменте с использованием этих функций получают следующее выражение:

$$\Delta z_{\text{риск}}^{\text{актив}} = \sum_{j=0}^N \int_0^{\Delta T} p_j(\Delta t) \Delta p(\Delta t) \Delta u(\Delta t) d(\Delta t) + \int_0^{\Delta L} \pi_j(\Delta l) \Delta \pi(\Delta l) \Delta v(\Delta l) d(\Delta l),$$

а ожидаемые рискованные потери —

$$\Delta z_{\text{риск}}^{\text{актив}} = \sum_{j=0}^N \int_0^{\Delta T} \tilde{p}_j(\Delta t) \Delta' z_j(\Delta t) d(\Delta t) + \sum_{j=0}^N \int_0^{\Delta L} \tilde{\pi}_j(\Delta l) \Delta' z_j(\Delta l) d(\Delta l).$$

В заключение следует отметить, что естественной областью приложения континуальной модели являются объекты (например, судовые двигатели), рискованные параметры которых по своей физической природе допускают непрерывное изменение (температура, напряжение и т. п.).

Результаты исследования и их обсуждение (Results and Discussion)

В результате исследования задачи управления рисками при разработке программных продуктов обслуживания информационных потоков на водном транспорте разработаны два подхода. В модели пассивного управления построена методика определения возможных рискованных потерь на основе как дискретного, так и континуального представления риск-факторов и соответствующих им вероятностей. В основе модели активного управления находится идея о возможном снижении суммарных рискованных потерь за счет целенаправленного изменения исходных вероятностей рисков, при условии, что снижение пассивной составляющей общих затрат / потерь превысит дополнительные затраты на указанное снижение.

В рамках исследования выполнено следующее:

- введены понятия пассивного и активного управления рисками;
- выделены два фактора риска, подверженные управлению в проектах разработки программного продукта: превышение планового размера кода и превышение планового срока исполнения;
- предложено количественное выражение для этих факторов в виде реперных точек в дискретной модели и в виде непрерывных функций в континуальной модели;
- предложены способы экспертного задания вероятностей факторов риска в виде дискретных либо, соответственно, непрерывных распределений;
- получены формулы для определения рискованных потерь при пассивном управлении и потерь / затрат при активном управлении.

В рамках изложенного подхода появляется возможность сравнения риск-менеджмента проекта с альтернативными вариантами снижения вероятности рисков по итоговому соотношению значений затрат на снижение вероятностей и меньших ожидаемых потерь при реализации рисков с полученными новыми вероятностями.

Заключение (Conclusion)

Управление рисками при разработке программных продуктов обслуживания информационных потоков на водном транспорте (в том числе связанных с информационной защитой) позволяет помимо традиционного оценивания потерь при реализации рисков превышения размеров кода и длительности исполнения использовать *активный подход*. Его базовой предпосылкой является представление о возможном снижении общих затрат на проект в случае, когда затраты на организационные мероприятия разработчика по снижению вероятностей риска окажутся меньше ожидаемого при этом снижения рискованных потерь.

Предложенная в статье методика, основанная на математическом моделировании процесса взаимодействия рискованных потерь, управленческих затрат и их итогового результата, позволяет использовать, как правило, несовпадающие экспертные оценки, выполненные средствами теоретико-вероятностного аппарата. При этом критериальные показатели качества риск-менеджмента выступают как математические ожидания вводимых в рассмотрение случайных величин — как дискретных, так и (при альтернативном подходе) непрерывных. Предложены способы расчета соответствующих затратных функций и сформулированы ограничения на них, вытекающие из вероятностной природы параметров модели. Указаны возможные области применения континуальных моделей в технических системах водного транспорта.

СПИСОК ЛИТЕРАТУРЫ

1. Демарко Т. Вальсируя с медведями: управление рисками в проекте при разработке программного обеспечения / Т. Демарко, Т. Листер. — М.: Компания р. m. Office, 2005. — 190 с.
2. Каретников В. В. К вопросу оценки рисков на внутреннем водном транспорте Российской Федерации / В. В. Каретников, К. И. Ефимов, А. А. Сикарев // Вестник Астраханского Государственного технического университета. Серия: Морская техника и технология. — 2017. — № 2. — С. 22–27. DOI: 10.24143/2073-1574-2017-2-22-27.
3. Anatoliy P. N. Aggregation process for implementation of application security management based on risk assessment / A. P. Nyrkov, Yu. F. Katorin, V. D. Gaskarov, Ya. V. Kosyak, A. V. Sauchev // 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). — IEEE, 2018. — Pp. 98–101. DOI: 10.1109/EIConRus.2018.8317039.
4. Холин А. И. Основные риски, связанные с разработкой программного обеспечения / А. И. Холин // Научный лидер. — 2023. — № 18 (116). — С. 43–44.
5. Тихонов А. Г. Управление рисками при разработке программного обеспечения / А. Г. Тихонов, Т. Н. Субботина // Экономика и бизнес: теория и практика. — 2022. — № 5–3 (87). — С. 122–125. DOI: 10.24412/2411-0450-2022-5-3-122-125.
6. Макаров Д. А. О факторах риска в процессе разработки программного обеспечения / Д. А. Макаров, М. Я. Розенберг, А. Б. Шильников // Вестник Южно-Уральского государственного университета. Серия: Математическое моделирование и программирование. — 2009. — № 37 (170). — С. 85–92.
7. Волошин И. П. Факторы риска при разработке программного обеспечения / И. П. Волошин // Информационная безопасность регионов. — 2016. — № 3 (24). — С. 15–19.
8. Каретников В. В. К вопросу оценки рисков использования безэкипажных средств водного транспорта на участке акватории / В. В. Каретников, С. В. Козик, А. А. Буцанец // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2019. — Т. 11. — № 6. — С. 987–1002. DOI: 10.21821/2309-5180-2019-11-6-987-1002.
9. Нырков А. П. Программно-аппаратная реализация системы предупреждения аварийной ситуации для объектов морского транспорта / А. П. Нырков, С. С. Соколов, А. А. Жиленков, С. Г. Черный // Автоматизация в промышленности. — 2016. — № 2. — С. 56–60.

10. Mamunts D. Models and algorithms for estimation and minimization of the risks associated with dredging / D. Mamunts, S. Sokolov, A. Nyrkov, S. Chernyi, M. Bukhurmetov, V. Kuznetsov // *Transport and Telecommunication*. — 2017. — Vol. 18. — No. 2. — Pp. 139–145. DOI: 10.1515/ttj-2017-0013.
11. Нырков А. П. Модели, алгоритмы и программное обеспечение минимизации рисков мультимодальных перевозок / А. П. Нырков, А. А. Нырков // *Вестник государственного университета морского и речного флота имени адмирала С. О. Макарова*. — 2013. — № 1 (20). — С. 67–73.
12. Nyrkov A. P. Hard- and Software Implementation of Emergency Prevention System for Maritime Transport / A. P. Nyrkov, A. A. Zhilenkov, S. S. Sokolov, S. G. Chernyi // *Automation and Remote Control*. — 2018. — Vol. 79. — Pp. 195–202. DOI: 10.1134/S0005117918010174.
13. Вихров Н. М. Анализ информационных рисков / Н. М. Вихров, А. П. Нырков, Ю. Ф. Каторин, А. А. Шнуренко, А. В. Башмаков, С. С. Соколов, Р. А. Нурдинов // *Морской вестник*. — 2015. — № 3 (55). — С. 81–85.
14. Veselkov V. Development of Methods to Identify Risks to Build up the Automated Diagnosis Systems / V. Veselkov, N. Vikhrov, A. Nyrkov, S. Chernyi, I. Titov // 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). — IEEE, 2017. — Pp. 598–601. DOI: 10.1109/EIConRus.2017.7910625.
15. Нырков А. П. Анализ и оценка рисков на водном транспорте / А. П. Нырков // Региональная информатика «РИ-2014»: Материалы XIV Санкт-Петербургской международной конференции. — СПб.: Санкт-Петербургское общество информатики, связи и управления, 2014. — С. 278–279.
16. Зак Ю. А. Принятие решений в условиях нечетких и размытых данных: Fuzzy-технологии / Ю. А. Зак. — М.: «ЛИБРОКОМ», 2013. — 352 с.
17. Function Point Counting Practices Manual. Release 4.2. — IFPUG, 2004.

REFERENCES

1. DeMarco, Tom, and Timothy Lister. *Waltzing With Bears: Managing Risk on Software Projects*. Dorset House, 2003.
2. Karetnikov, V. V., K. I. Efimov, and A. A. Sikarev. “To the question of risk assessment on domestic water transport of the Russian Federation.” *Vestnik of Astrakhan State Technical University. Series: Marine engineering and technologies* 2 (2017): 22–27. DOI: 10.24143/2073-1574-2017-2-22-27.
3. Nyrkov, Anatoliy P., Yuri F. Katorin, Vagiz D. Gaskarov, Yana V. Kosyak, and Aleksandr V. Sauchev. “Aggregation process for implementation of application security management based on risk assessment.” *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 2018. 98–101. DOI: 10.1109/EIConRus.2018.8317039.
4. Kholin, A.I. “Main risks associated with software development.” *Nauchnyi lider* 18(116) (2023): 43–44.
5. Tikhonov, A.G., and T. N. Subbotina. “Risk management in software development.” *Economy and Business* 5–3(87) (2022): 122–125. DOI: 10.24412/2411-0450-2022-5-3-122-125.
6. Makarov, D.A., M. Y. Rozenberg, and A. B. Shilnikov. “Risks in software development process.” *Bulletin of the South Ural State University, Series “Mathematical Modelling, Programming & Computer Software”* 37(170) (2009): 85–92.
7. Voloshin, I.P. “Risk factors in the development of software.” *Informatsionnaya bezopasnost' regionov* 3(24) (2016): 15–19.
8. Karetnikov, Vladimir V., Sergey V. Kozik, and Artem A. Butsanets. “Risks assessment of applying unmanned means of water transport in the water area.” *Vestnik Gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S. O. Makarova* 11.6 (2019): 987–1002. DOI: 10.21821/2309-5180-2019-11-6-987-1002.
9. Nyrkov, A. P., S. S. Sokolov, A. A. Zhilenkov, and S. G. Chernyi. “Programmno-apparatnaya realizatsiya sistemy preduprezhdeniya avariinoy situatsii dlya ob'ektov morskogo transporta.” *Avtomatizatsiya v promyshlennosti* 2 (2016): 56–60.
10. Mamunts, D., S. Sokolov, A. Nyrkov, S. Chernyi, M. Bukhurmetov, and V. Kuznetsov. “Models and algorithms for estimation and minimization of the risks associated with dredging.” *Transport and Telecommunication* 18.2 (2017): 139–145. DOI: 10.1515/ttj-2017-0013.
11. Nyrkov, A. P., and A. A. Nyrkov. “Modeli, algoritmy i programnoe obespechenie minimizatsii riskov mul'timodal'nykh perevozk.” *Vestnik gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S. O. Makarova* 1(20) (2013): 67–73.

12. Nyrkov, Anatoliy P., A. A. Zhilenkov, S. S. Sokolov, and S. G. Chernyi. "Hard-and software implementation of emergency prevention system for maritime transport." *Automation and Remote Control* 79 (2018): 195–202. DOI: 10.1134/S0005117918010174.
13. Vikhrov, N. M., A. P. Nyrkov, Yu. F. Katorin, A. A. Shnurenko, A. V. Bashmakov, S. S. Sokolov, and R. A. Nurdinov. "Analiz informatsionnykh riskov." *Morskoi vestnik* 3(55) (2015): 81–85.
14. Veselkov, Viacheslav, Nikolai Vikhrov, Anatolii Nyrkov, Sergei Chernyi, and Ivan Titov. "Development of methods to identify risks to build up the automated diagnosis systems." *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 2017. 598–601. DOI: 10.1109/EIConRus.2017.7910625.
15. Nyrkov, A. P. "Analiz i otsenka riskov na vodnom transporte." *Regional'naya informatika "RI-2014". Materialy XIV Sankt-Peterburgskoi mezhdunarodnoi konferentsii*. SPb.: Sankt-peterburgskoe obshchestvo informatiki, svyazi i upravleniya, 2014. 278–279.
16. Zak, Yu. A. *Prinyatie reshenii v usloviyakh nechetkikh i razmytykh dannykh: Fuzzy-tehnologii*. M.: «LIBROKOM», 2013.
17. *Function Point Counting Practices Manual*. Release 4.2. IFPUG, 2004.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Ястребов Иван Михайлович —
инженер по разработке ПО
ООО «ЯДРО ЦЕНТР ПРОГРАММНЫХ
РАЗРАБОТОК»
193376, Российская Федерация, Москва,
ул. Рочдельская, 15, стр. 15
e-mail: vanka998@mail.ru

INFORMATION ABOUT THE AUTHOR

Yastrebov, Ivan M. —
Software development engineer
YADRO SOFTWARE DEVELOPMENT CENTER,
LLC.
15 Rochdelskaya Str., Moscow, 193376,
Russian Federation
e-mail: vanka998@mail.ru

*Статья поступила в редакцию 15 ноября 2023 г.
Received: November 15, 2023.*