

ПРОБЛЕМЫ АНАЛИЗА И ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Смирнов А.А.

*доктор технических наук, профессор,
зав. каф. программирования и защиты информации
Кировоградский национальный технический университет,
dr.smirnova@gmail.com, http://it-kntu.kr.ua/*

Коваленко А.В.

*кандидат технических наук, доцент
доц. каф. программирования и защиты информации
Кировоградский национальный технический университет*

Аннотация. *Рассматриваются проблемы анализа и оценки рисков информационной деятельности. Определена общая последовательность оценки рисков чаще всего включает в себя следующие действия.*

Всеобщие процессы глобализации экономических, финансовых, социальных и информационных отношений способствовали развитию направления риск-менеджмента. Однако общемировые финансовые кризисы показали недостаточно внимательное отношение к управлению рисками со стороны большинства представителей руководства организаций, в том числе и в Украине. В настоящее время в большинстве организаций и предприятий различных форм собственности все больше внимания уделяется вопросам анализа и оценки рисков. Но, несмотря на это проблемы и вопросы, относящиеся к общей теории и методологии анализа, оценки и управления рисками требуют адаптации к подходам и положениям современного менеджмента, учета новых факторов становления и развития технологий, объединения известных «устоявшихся» положений теории рисков с новыми, прогрессирующими подходами анализа и синтеза.

Проведенный анализ литературы показал, что несмотря на достаточно глубокую историю развития понятия «риск» и попытки ряда известных авторов сконцентрировать свои разработки в область управления рисками отдельных отраслей и направлений деятельности, разработка новых, перспективных научных положений в этой области все же несколько «заужена» финансовой деятельностью. В то же время широкое использование в нашей работе информационных технологий требует повышенного внимания к этому направлению, и соответственно, более глубокого освещения вопросов риск-менеджмента IT-индустрии.

Следует заметить, что объективный результат является следствием целенаправленного и явного выполнения процесса, который связан с его сутью. Субъективные результаты проявляются в тех случаях, когда выполнение процесса проходит с недостаточным уровнем определенности и полноты информации. На практике в сфере IT-индустрии, преобладающее количество рисков связаны именно с субъективными результатами осуществления хода или выполнения процесса.

Получение необходимой информации связано с наличием четких и определенных (стандартизированных, апробированных, регламентированных и т.д.) средств, инструментов, методов и методик, выполнение которых связано с ресурсными затратами, а также отсутствием достоверных данных о цели и сущности исследуемого процесса.

Таким образом, можно отметить, что все риски при разработке программного обеспечения, с большим или меньшим допущением, можно считать субъективным результатом выполнения процесса, который связан с недостатком количественной или качественной информации о процессе, а также ее неопределенностью. Указанные факторы можно считать главной причиной, которая порождает и сопровождает риски, во всем их жизненном цикле.

Каждый риск цикла разработки программного обеспечения (ПО) можно связать с одним из следующих компонентов: данные; человек; система. При этом следует учесть

степень влияния и ответственности результатов оценки рисков для разных методологий разработки программного обеспечения.

Анализ литературы показал, что в настоящее время существует множество $R = \{x_1, K, x_n\}$ различных методик разработки ПО. Следует заметить, что выбор непосредственно методики при реализации проекта оказывает существенное влияние на результаты анализа, оценки и управления рисками. Например, из литературы известно, что одной из широко используемых методологий разработки ПО является спиральная методология. Предложенная в 1988 году американским специалистом Барри Бом (Barry Boehm) эта методология руководствуется инкрементными разработками на основе рисков. Более 15% временных затрат управления IT-проектами уходит на анализ и оценку рисков. При этом следует заметить, что на каждом витке «спирали» данная задача имеет свои особенности и ограничения, оказывающие влияние на процесс управления рисками в системе. Анализ литературы показал, что современные авторы в своем большинстве выделяют пять основных рисков: ошибки, присущие расписанию, появление новых требований, смена сотрудников, декомпозиция спецификации, низкая продуктивность.

Проведенные исследования показали, что данная позиция спорна, поскольку не учитывает ряд важных аспектов разработки ПО. Анализ нормативной документации ряда известных фирм-разработчиков ПО показал, что на этапе оценки рисков, как правило, не учитываются риски, связанные с возможным наличием ошибок в моделях, алгоритмах, программах обработки информации, которые используются для выработки управляющих решений, пренебрегаются риски безопасности (возможных ошибок влияющих на уязвимость ПО). Это зачастую приводит к ошибкам и соответственно необоснованным потерям (временным, экономическим, имиджевым и др.).

Таким образом, проведенные исследования показали, что, несмотря на важность решения задачи управления рисками при разработке ПО, на данный момент нет четко сформированной, стандартизированной методологической базы описания данного процесса. В настоящее время наблюдается:

- отсутствие единого, комплексного и системного подхода на проблему возникновения рисков при разработке ПО;
- отсутствие ясности и прозрачности в понимании конечных результатов воздействия рисков, их недостаточного учета, при разработке ПО;
- значительные разночтения в понимании методик анализа, оценки и управления рисками;
- недостаточность учета важных факторов, возникающих по мере совершенствования технологий и средств разработки ПО.

Анализ литературы и проведенные исследования показали, что общая последовательность оценки рисков чаще всего включает в себя следующие действия:

1. Выявление источников и причин риска разработки ПО, этапов и работ, при выполнении которых возникает риск.
2. Идентификация всех возможных рисков, свойственных рассматриваемому проекту.
3. Документирование результатов и их последующая приоритезация.
4. Оценка уровня отдельных рисков и риска проекта в целом, определяющая его экономическую целесообразность.
5. Определение допустимого уровня риска разработки ПО.
6. Разработка мероприятий по снижению риска.

В соответствии с данным алгоритмом оценка риска подразделяется на три взаимно дополняющих направления: качественный (этапы 1, 2, 3) и количественный анализ (этапы 4, 5) рисков разработки ПО, а также управление (этап 6).

Поэтому в дальнейшем необходимо исследовать более подробно методики качественного и количественного анализа рисков разработки ПО.