УДК 004.41:004.056

А.А. Смирнов, А.В. Коваленко, Н.Н. Якименко, А.П. Доренский

Кировоградский национальный технический университет, Кировоград

ПРОБЛЕМЫ АНАЛИЗА И ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

Данная статья посвящена формированию проблемы анализа и оценки рисков информационной деятельности в рамках комплекса методов качественного анализа и количественной оценки рисков разработки программного обеспечения, что позволило решить противоречие, возникающих при разработке программного обеспечения, и заключающееся в пренебрежении фирмами-разработчиками программного обеспечения факторов уязвимости безопасности программного обеспечения.

Ключевые слова: *оценка рисков, разработка программного обеспечения.*

Постановка проблемы исследования

Авторами разработан комплекс методов качественного анализа и количественной оценки рисков разработки программного обеспечения, что позволило решить противоречие, возникающих при разработке программного обеспечения (ПО), и заключающееся в пренебрежении фирмами-разработчиками ПО факторов уязвимости безопасности ПО. В качестве решения указанной проблемы предложено использование разработанных методов качественного анализа и количественной оценки рисков разработки программного обеспечения. Данная статья посвящена формированию проблемы анализа и оценки рисков информационной деятельности.

Основная часть

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.

Анализ литературы [1 – 13] 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 «зауже-на» 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.

Сутью любого процесса, явления или объекта (в том числе и информационной составляющей) является деятельность, которая приводит к формированию результатов. В приложении к такому направлению деятельности, как разработка программного обеспечения, конечным результатом, в большинстве практических случаев, является выполнение требований заказчика и внедрение разработанного продукта. Современные авторы [1 – 13] очень часто результат оцениваемого риска сводят к отрицательному типу эффекта, забывая, что даже сам термин «риск» произошел от французского слова «risqué» или итальянского «risico». Оно означает возможность или вероятность наступления событий с конкретными последствиями в результате определенных решений или действий. Целесообразность такого представления понятий в теории риска особенно подчеркивается закономерностями, возникающими в информационных отношениях при разработке программного обеспечения, где сложность и динамика взаимосвязей, нечеткость внешних факторов, а также гетерогенность в структурном и функциональном построении систем позволяет расширить классификацию результатов информационной деятельности до вида, представленного на рис. 1. 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.

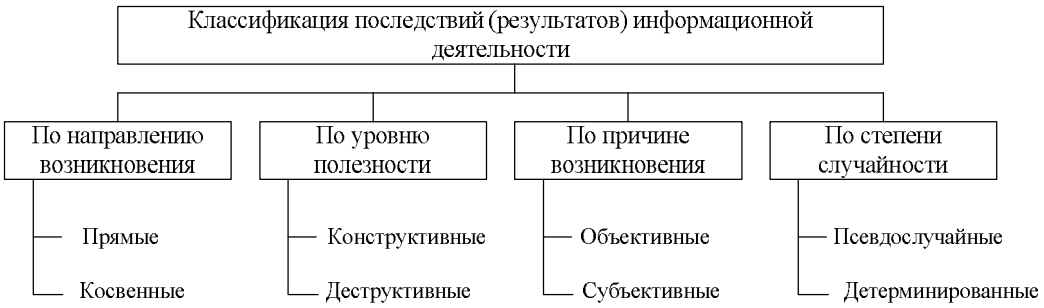

Рис. 1. Классификация результатов информационной деятельности

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 [1 – 13] показал, что в настоящее время существует множество $R = \{x_1, \ldots, x_n\}$ 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 [6] известно, что одной из широко используемых методологий разработки ПО является спиральная методология. Предложенная в 1988 году американским специалистом Барри Бом (Barry Boehm) [6] эта методология руководствуется инкрементными разработками на основе рисков (рис 2).

Как видно из рис. 2. 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 [1 – 13] 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: отсутст-

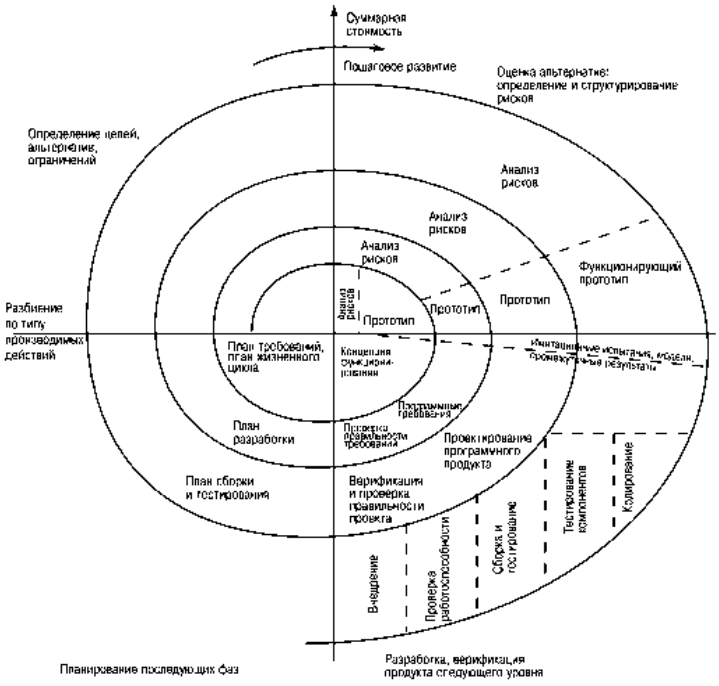

Рис. 2. Спиральная методика разработки ПО [6]

вие 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 [1 – 13] и проведенные исследования показали, что общая последовательность оценки рисков чаще всего включает в себя следующие действия: 1) ыявление 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).

Выводы

Таким образом, в работе определено и решено одно из противоречий, возникающих при разработке ПО, и заключающееся в пренебрежении фирмами-разработчиками ПО факторов уязвимости безопасности ПО. В качестве решения указанной проблемы предложено использование разработанных методов качественного анализа и количественной оценки рисков разработки программного обеспечения.

Список литературы

1. Krishnan M. Soumya Software Development Risk Aspects and Success Frequency on Spiral and Agile Model / M. Soumya Krishnan // International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015 pp.301-310

2. Zeng Y. Risk Management For Enterprise Resource Planning System Implementations in Project-Based Firms : dis. for the degree of PHD / Zeng Yajun, Maryland, 2010 – P. 210.

3. Бриткин А. И. Риски, связанные с внедрением технологий, в проектах разработки программного обеспечения / А. Бриткин // Социально-экономические и технические системы. – 2007. – № 8 (42)

4. Вишняков Я.Д Общая теория рисков: учеб. пособие для студ. высш. учеб. заведений / Я.Д.Вишняков, Н.Н.Радаев. – М. : Изд. центр «Академия», 2008. – 368 с.

5. Шапкин А.С. Теория риска и моделирование рисковых ситуаций / А.С. Шапкин, В.А. Шапкиню.– М.: «Дашкв и К», 2005. – 880 с.

6. Boehm B.W. A spiral model of software development and enhancement / Boehm B., Egyed A. // IEEE Computer, May 1988 pp. 61-72

7. Исикава К. Японские методы управления качеством / К. Исикава, Сокр.пер. с англ. / Под. Ред. А. В. Гличева. — М: Экономика, 1988. — 214 с.

8. Інженерія програмного забезпечення: Навч. посібник / [Смірнов О.А., Коваленко О.В., Мелешко Є.В. та ін.] – К.: РВЛ КНТУ, 2013. – 409 с.

9. Доренський О.П. Формалізація процесу зміни станів програмних об'єктів складних систем на основі формального апарату скінченних автоматів Мура / О.П. Доренський, О.А. Смірнов // Зв'язок. – 2014. – № 3 (109).— С. 27-31.

10. Dorensky O. Development of the theoretical bases of logical domain modeling of a complex software system / O/ Dorensky, Al. Smirnov // Int. Journal of Comp. Eng. Research (IJCER). – India: Delhi, 2014. — Vol. 4, Is. 4. — P. 19-23

11. Лысенко И.А. Исследование уровней тестирования программного обеспечения инфотелекоммуникационных систем / И.А. Лысенко, А.А. Смирнов, Е.В. Мелешко // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Харків: ХУПС. – 2014. – С.79-81.

12. Лысенко И.А. Исследование процесса разработки программного обеспечения инфотелекоммуникационных систем / И.А. Лысенко, А.А. Смирнов, Л.И Полищук // Системи озброєння і військова техніка. – Випуск 4(40) – Х.: ХУПС – 2014. – С. 103-106.

13. Лысенко И.А. Исследование алгоритма выявления вида неучтенных тестовых случаев в процессе проектирования тестовых наборов / И.А. Лысенко, А.А. Смирнов // Зв'язок. – К. ДУТ, 2014. - № 2 (108) . – С. 153-156.

Поступила в редколлегию 29.01.2016

Рецензент: д-р техн. наук, ст. научн. сотр. С.Г. Семенов, Национальный технический университет «ХПИ», Харьков.

ПРОБЛЕМИ АНАЛІЗУ І ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

О.А. Смірнов, О.В. Коваленко, Н.М. Якименко, О.П. Доренський

Дана стаття присвячена формуванню проблеми аналізу та оцінки ризиків інформаційної діяльності в рамках комплексу методів якісного аналізу та кількісної оцінки ризиків розробки програмного забезпечення, що дозволило вирішити протиріччя, які виникають при розробці програмного забезпечення, і що полягає в нехтуванні фірмами-розробниками програмного забезпечення чинників вразливості безпеки програмного забезпечення.

Ключові слова: *оцінка ризиків, розробка програмного забезпечення.*

PROBLEMS ANALYSIS AND RISK ASSESSMENT INFORMATION ACTIVITIES

A.A. Smirnov, A.V. Kovalenko, N.M. Yakimenko, O.P. Dorensky

This article deals with the formation of the problem analysis and risk assessment information activities within the complex methods of qualitative analysis and quantitative assessment of the risks of software development, which resolves the contradiction arising from the development of software, and which consists in neglecting the companies-software developers factors of software security vulnerabilities.

Keywords: *risk assessment, software development.*