2. Lyu M. R. Handbook of Software Reliability Engineering. IEE Computer Society Press and McGraw – Hill Book Company, 1996, 819 p.

3. Lyu M. R. Software Fault Tolerance. John Wiley& Sons Ltd, 1996.

4. Kovalev I. V., Zav'jalova O. I., Lajkov A. N. [Formation of excessive soft-ware fault-tolerant control systems]. *Izvestija vysshikh uchebnykh zavedenij*. *Priborostroenie.* 2008, Vol. 51, no. 10, p. 30–34. (In Russ.)

5. Kovalev I. V., Junusov R. V. [Multiversioning-tion method for increasing software reliability information-communication technologies in corporate structures]. *Distantsionnoe i virtual'noe obuchenie.* 2003, no. 2, p. 50–55. (In Russ.)

6. Carev R. Ju. [Multiversioning approach to an increase resiliency of software program management systems and information processing]. *V mire otkrytij.* 2010, vol 10, no. 4, Ch. 10, p. 82–84. (In Russ.)

7. Kovalev I. V., Slobodin M. Ju., Stupina A. A. [Mathematical problem of designing N-versioned software systems]. *Problemy mashinostroenija i avtomatizatsii*. 2005, no. 3, p. 16–23. (In Russ.)

8. Kovalev I. V., Stupina A. A., Carev R. Ju., Volkov V. A. [Application of COM technology for realizations multiversioning soft-ware systems, control and information processing]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika.* 2007, no. 3, p. 18–22. (In Russ.)

9. Kovalev I. V., Novoj A. V., Shtancel' A. V. [Evaluation of reliability multiversioning software architecture of management systems and information processing]. *Vestnik SibGAU.* 2008, vol. 20, no. 3, p. 50–52. (In Russ.)

10. Kovalev I. V., Novoj A. V. [Calculation of reliability of fault-tolerant software architectures]. *Vestnik SibGAU.* 2007, vol. 17, no. 4, p. 14–17. (In Russ.)

11. Kovalev I. V., Dgioeva N. N., Slobodin M. Ju. The mathematical system model for the problem of multiversion software design. *Proceedings of Modelling and Simulation, MS'2004* AMSE International Conference on Modelling and Simulation, MS'2004. Lyon-Villeurbanne, 2004.

12. Marco Dorigo, Thomas Stutzle. Ant Colony Optimization. *Massachusetts Institute of Technology,* 2004.

13. Dorigo M., Maniezzo V., Colorni A. The Ant System: An Autocatalytic Optimizing Process. Technical Report no. 91-016 Revised, Politecnico di Milano, Italy, 1991, 103 p.

14. Colorni A., M. Dorigo, V. Maniezzo An Inverstigation of Some Properties of an Ant Algorithm. *Proceedings of the Parallel Problem Solving from Nature Conference* (PPSN 92). Brussels, Beldium, R. Manner and B. Manderick (Eds.), Elsevier Publishing. 1992, p. 509–520.

15. Kovalev I. V., Solov'ev E. V., Kovalev D. I., Bahmareva K. K., Demsish A. V. [The use of particle swarm to form the composition of the multiverse-onnogo software]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika,* 2013, no. 3, p. 1–6. (In Russ.)

16. Corne D, Dorigo M, Glover F New Ideas in Optimization. McGrav – Hill. 1999, 314 p.

17. Shtovba S. D. [Ant algorithms]. *Matematika v prilozhenijah*. 2003, no. 4 (4), p. 70–75. (In Russ.)

18. Kovalev I. V., Karaseva M. V., Solov'ev E. V. [Modification of the ant algorithm to the problem of forming multiversioning software]. *Vestnik SibGAU.* 2014, vol. 53, no. 1, p. 19–24. (In Russ.)

19. Kovalev I. V., Carev R. Ju., Prokopenko A. V., Solov'ev E. V. [On the Implementation of the ant algorithm for choosing the composition multiversioning software information management systems]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika.* 2012, no. 2, p. 1–4. (In Russ.)

20. Kul'ba V. V., Mikrin E. A., Pavlov B. V. *Prektirovanie informatsionno-upravljajushhikh sistem dolgovremennykh orbital'nyh stantsij* [Design of information management systems of long-term orbital stations]. Moscow, Nauka Publ., 2002, 343 p.

УДК 004.056

МЕТОДИКА АНАЛИЗА И ОЦЕНКИ РИСКОВ ОРГАНИЗАЦИИ

И. З. Краснов[1], О. И. Карелин[2]

[1]Сибирский федеральный университет
Российская Федерация, 660041, г. Красноярск, просп. Свободный, 79
[2]Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Российская Федерация, 660014, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: bk_24@bk.ru, karelin@sibsau.ru

Стремительное развитие компьютерной сферы и высоких технологий в последние два десятилетия привело к тому, что информация приобрела конкретные финансовые, репутационные, временные и экономические выражения. В связи с этим для большинства организаций защита информации становится одной из приоритетных задач.

Статья посвящена вопросам анализа информационных рисков. Приводится методика оценки и распределения информационных рисков. Выделены уровни информационной безопасности в соответствии с глубиной детализации карт бизнес-процессов в контексте важных информационных активов организации. Особое внимание уделяется распределению ответственности за оценку и учет информационных рисков, приводится методика многоуровневой оценки конечных рисков организации с учетом размеров и производственных характеристик организации. Одним из первых и основных этапов построения защищенной инфраструктуры организации является анализ оценки защищенности информационной системы.

Ключевые слова: информационная безопасность, информационные риски, многоуровневая оценка рисков, стабильность информационной системы предприятия, модель системы защиты информации.

INFORMATION RISK MANAGEMENT

I. Z. Krasnov[1], O. I. Karelin[2]

[1]Siberian Federal University
79, Svobodny prosp., Krasnoyarsk, 660041, Russian Federation
[2]Siberian State Aerospace University named after academician M. F. Reshetnev
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660014, Russian Federation
E-mail: bk_24@bk.ru, karelin@sibsau.ru

The article is devoted to information risk management. The authors gives an assess and distribution technique of information risks. Levels of information security is considered in the context of information asset relevance for organization objectives and granularity of bushiness process maps. Particular attention is paid to the distribution of responsibility for evaluating and recording the information risk. A multi-level evaluation methodology for end-risks the organization with the size and characteristics of the business is offered. An information system security analysis is the first and one of the most important steps of stable infrastructure constructing.

Keywords: information security, information risk, multi-level risk assessment, stability of the IT company, information security system model.

В рамках данной статьи под целевой аудиторией будем понимать российские компании, которые используют информационные технологии при ведении основного бизнес-процесса, информационные технологии (ИТ) для капитализации производства, а также организации, для которых информационная борьба является одним из механизмов, позволяющих оставаться конкурентоспособными на международном рынке.

Рассмотрим, какими свойствами должна обладать методика анализа и оценки рисков организации:

– простота понимания руководством и сотрудниками;

– малые трудозатраты на реализацию и эксплуатацию;

– гибкость, позволяющая модифицировать реализацию вместе с ростом или уменьшением организации;

– возможность непрерывного мониторинга;

– возможность интеграции в корпоративную систему ИБ, основанную на процессном подходе;

– удовлетворение требованиям международных стандартов;

– учет человеческого фактора;

– отказоустойчивость.

Риск-ориентированный подход лежит в основе современного корпоративного управления. Оценка рисков позволяет принимать осознанные решения, правильно выбирая механизмы защиты и расставляя приоритеты. Оценка рисков позволяет избегать многих кризисных ситуаций. После кризиса остаются те, кто правильно управлял рисками.

Все современные стандарты и руководства в области корпоративного управления, включая стандарты на интегрированные системы управления (PAS 99), стандарты СУИБ (ISO 27001), банковские стандарты (СТО БР ИББС и Basel II), а также нормативные требования, предъявляемые к публичным компаниям (Turnbull и SoX), базируются на оценке рисков. Риски информационной безопасности следует рассматривать как неотъемлемую часть рисков всего бизнеса [1, с. 56].

Рассматривая малые и средние организации на российском рынке, стоит отметить их многообразие, связанное с большим количеством различных культур и экономических условий, а соответственно, и потребностей. Среди существующих продуктов для анализа рисков почти для любой организации возможно найти продукт с рядом достоинств и преимуществ, но универсального продукта на сегодняшний день не существует.

Системы ГРИФ, «Кондор», RiskWatch имеют ряд достоинств, но отсутствие качественного расчета риска не позволяет им удовлетворять критерию «простота понимания руководством и сотрудниками» в связи с недостаточно глубоким пониманием руководством компаний всей значимости расчета рисков с целью создания защищенного информационного поля, определив контур информационной безопасности (ИБ). Руководству организации будет намного удобнее воспринимать качественную оценку риска, чем полученные количественным способом расчетные финансовые средства, которые организация не получает в виде прибыли.

Методики CRAMM и RiskWatch требуют больших трудозатрат на реализацию и поддержание системы, а малое количество специалистов в данной области усугубляет ситуацию.

Методика CORAS не пригодная для постоянного мониторинга рисков ИБ. Ее использование целесообразно для разового расчета рисков и определения реальной картины в настоящий момент.

Методика FRAP не учитывает человеческий фактор, имеет слабый механизм мониторинга и требует большое количество статистических данных, что затрудняет развертывание системы в организациях.

Методика OCTAVE реализована в виде конечного числа продуктов, нацеленных на разные организации. При модернизации организации, даже оставаясь на данной системе, требуются большие изменения. Также методика не учитывает рекомендации, предъявляемые к человеческому фактору в соответствии с международными стандартами информационной безопасности ISO 15408, 27001, а также требования стандарта COBIT (методика управления, контроля и аудита информационных систем).

Его новая версия COBIT5 рассматривает 7 факторов влияния (enablers) на систему ИТ (ИБ): принципы, политики и подходы, процессы; организационная структура; персонал, навыки и компетенции; культура; этика и поведение; информация; услуги, инфраструктура и приложения.

Из этого следует, что на данный момент не существует универсальной методики, которая бы подходила целевой аудитории. А наличие таковой важно, так как до сих пор некоторые руководители не понимают важности работ по оценке рисков в их организациях, в том числе и по причине неполного совершенства существующих на рынке информационной безопасности программ [2, с. 4].

Решить данные проблемы предлагается путем построения многоуровневой карты бизнес-процессов организации. На рис. 1 показано построение карты бизнес-процессов.

При построении процесс разбивается на несколько подпроцессов – от 2 до 10. Можно выделять более 12 подпроцессов, если приходится вводить дополнительные формальные уровни иерархии. На практике бывает удобно показывать при построении 10–12 подпроцессов. Это в основном касается описания процессов на средних и нижних уровнях. Таким образом, мы получим систему, которая учитывает особенности ведения деятельности организации на разных уровнях управления [3, с. 23].

В зависимости от глубины детализации карты можно получить информацию об активах с различной точностью, что позволяет данному методу быть применимым для организаций различных размеров и направлений деятельности, что является необходимым условием в рамках существующей целевой аудитории. Иерархическая система, состоящая из 4 уровней детализации, позволяет с большей точностью оценивать риски для важных активов и с меньшей – для маловажных.

После получения карт бизнес-процессов всех уровней необходимо идентифицировать активы, используемые процессами.

С точки зрения риск-ориентированного подхода, ведение деятельности обеспечивают активы организации. Идентификация активов позволяет определить, какая информация и как она обрабатывается в организации. Благодаря идентификации можно определить активы, необходимые для выполнения задач, и активы, которые усложняют выполнение таковых, замедляя процесс обработки информации [4, с. 23].

Выведение из пользования активов, не нацеленных на выполнение задач организации, существенно уменьшает уровень вероятности рисков организации. Определение необходимых активов позволяет сократить затраты на обеспечение информационной безопасности и на содержание активов.

Идентифицируя и описывая каждый актив, мы формируем таблицу активов организации:

– бизнес-процессов;
– информационных активов;
– кадровых ресурсов;
– аппаратных программных средств;
– каналов передачи информации.

Идентификацию активов следует начинать сверху вниз, т. е. с идентификации и описания бизнес-процессов, а не снизу вверх, формируя ни к чему не привязанные списки информационных, программных и аппаратных активов.

Бизнес-процессы сами по себе рассматриваются в качестве основных активов организации, которые представляют собой комбинацию разнородных активов, таких как информация, технические и программные средства, кадровые ресурсы и т. п. Все эти активы представляют ценность для организации только в контексте ее бизнес-процессов, в рамках которых они используются для достижения целей организации.

Идентифицировать и локализовать информацию можно на основании описания бизнес-процессов, в рамках которых информация рассматривается как один из типов ресурсов. Задача несколько упрощается, если в организации принят подход регламентации бизнес-деятельности (например, в целях управления качеством и оптимизации бизнес-процессов). Формализованные описания бизнес-процессов служат основной точкой отсчета для инвентаризации активов.

Активы – это все, что имеет ценность или находит полезное применение для организации, ее деловых операций и обеспечения их непрерывности. Поэтому активы нуждаются в защите для того, чтобы обеспечить корректность деловых операций и непрерывность бизнеса. Надлежащее управление и учет активов должны являться одной из основных обязанностей руководителей всех уровней [4, с. 109].

Идентификация и определение ценности активов, исходя из потребностей деятельности организации, являются основными факторами в оценке риска. Для того чтобы определить требуемый уровень защиты активов, необходимо определить их ценность с точки зрения их важности для организации. Учитываются законодательные требования, требования стандартов и корпоративных требований организации, а также последствия нарушения конфиденциальности, целостности и доступности этих активов.

Важность для активов определяется в соответствии с табл. 1.

При проведении анализа рисков организации следует начинать с низшего уровня и постепенно подниматься до основного процесса ведения бизнеса. Но данный процесс достаточно трудоемкий и затратный. Чтобы обеспечить простоту реализации данной методики, необходимо распределить ответственность за активы.

Нельзя обеспечить адекватный уровень информационной безопасности без установления подотчетности за активы. Для каждого из идентифицированных активов или группы активов должен быть определен владелец, на которого возлагается ответственность за осуществление контроля производства, разработки, сопровождения, использования и безопасности этих активов. Обязанности по внедрению механизмов безопасности могут быть делегированы, однако ответственность должна оставаться за назначенным владельцем актива [4, с. 109].

Важность для уровней бизнес-процессов ранжируется в соответствии с табл. 2.

Только благодаря адекватной оценке важности доверенных активов можно определить, какая угроза наиболее критична для всей организации. Для определения критичности угрозы необходимо проанализировать ее на всех уровнях управления, отследив цепочку принадлежности актива бизнес-процессам. Например, пусть аналогичная угроза присуща активам «А» и «Б» (рис. 2).

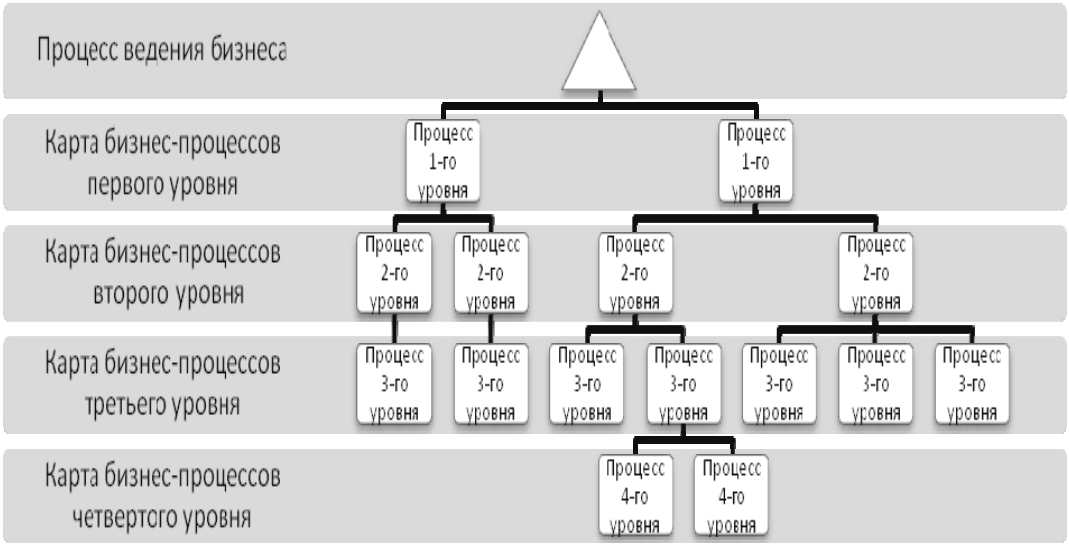

Рис. 1. Построение карты бизнес-процессов организации

Таблица 1

Возможные значения важности актива

Уровень важности	Описание
Особой важности	Кратковременное прерывание в работе актива приводит к существенному ущербу для бизнес-процесса, потере временного или качественного ресурса
Важный	Остановка актива приводит к существенному ущербу для бизнес-процесса, потере временного или качественного ресурса
Средней важности	Кратковременное прерывание в работе актива приводит к ограниченным временным или качественным потерям
Маловажный	Остановка актива приводит к ограниченным временным или качественным потерям
Неважный	Перерыв в работе актива не вызывает существенных потерь

Таблица 2

Возможные значения важности бизнес-процесса

Уровень важности	Описание
Особой важности	Кратковременное прерывание бизнес-процесса приводит к существенному ущербу для организации, потере временного или технологического ресурса
Важный	Остановка бизнес-процесса приводит к существенному ущербу для организации, потере временного или технологического ресурса
Средней важности	Кратковременное прерывание бизнес-процесса приводит к ограниченным временным или качественным потерям
Маловажный	Остановка бизнес-процесса приводит к ограниченным временным или качественным потерям
Неважный	Перерыв в работе бизнес-процесса не вызывает существенных потерь

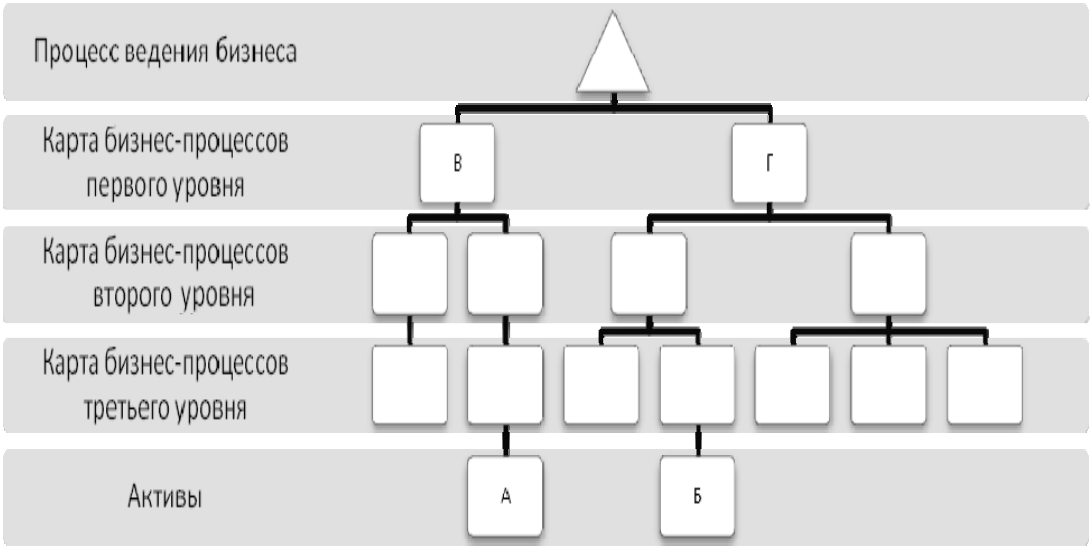

Рис. 2. Определение критичности угрозы

Предположим, что все процессы третьего уровня одинаково важны для соответствующих процессов второго уровня. В свою очередь, все процессы второго уровня одинаково важны для процессов «В» и «Г». Но процесс «В» выполняет основную задачу организации, а «Г» – вспомогательную. Исходя из вышеизложенного, процесс «В» является важнее для бизнеса, чем процесс «Г». Таким образом, мы приходим к выводу, что наиболее критичная из двух аналогичных угроз, присущих активам «А» и «Б», является угроза активу «А». Именно на эту угрозу следует обратить внимание в первую очередь, так как ее реализация критично повлияет на непрерывность ведения деятельности организации.

В реальной же ситуации многоуровневая карта бизнес-процессов намного больше, а каждый актив подвергается множеству угроз, и необходимо определять, какая из них будет влиять на бизнес сильнее. Поэтому владелец ресурса определяет, какие последствия несет реализация какой-либо угрозы, а владелец вышестоящего процесса определяет ущерб, который он понесет вследствие успешной реализации.

Для оценки вероятности реализации угрозы была использована следующая карта бизнес-процессов торгово-ориентированного предприятия.

Система деятельности организации предназначена для автоматизации процесса продаж и обеспечения финансово-хозяйственной деятельности, а именно:

– обеспечение сотрудников надежным доступом к внутренним и внешним ресурсам организации в соответствии с установленным регламентом;

– обеспечение своевременного предоставления всей необходимой и достоверной информации при взаимодействии с партнерами;

– предоставление качественного доступа к информационно-вычислительным ресурсам всем структурным подразделениям и отделам головного офиса.

Основная задача деятельности предприятия – обеспечить:

– сбор, обработку и предоставление доступа к информации законным пользователям;

– целостность и конфиденциальность информации, циркулирующей в информационно-вычислительной системе организации;

– доступ законным пользователям информационно-вычислительной системы организации;

– бесперебойную работу персональных рабочих станций и сетевого оборудования в офисе организации;

– сбор и надлежащее хранение информации, необходимой для расследования инцидентов с участием информационно-вычислительных ресурсов;

– соблюдение требований нормативно-правовых документов по ограничению устанавливаемого программного обеспечения на рабочие компьютеры офиса;

– контроль программно-аппаратной среды рабочих компьютеров в офисе организации;

– поддержание информационно-вычислительной системы в защищенном состоянии в соответствии с установленным регламентом.

В организации сформированы следующие подпространства пространства активов:

– подпространство бизнес-процессов;

– подпространство информационных активов;

– подпространство кадровых ресурсов;

– подпространство аппаратных средств;

– подпространство программных средств;

– подпространство каналов передачи информации.

Следует отметить, что каждые из вышеуказанных подпространств рассматриваются отдельно. В данной статье рассмотрено лишь подпространство бизнес-процессов.

Определим критичность угроз информационной безопасности к таким активам предприятия, как технические регламенты и программно-аппаратные комплексы для обеспечения технологического процесса. Потеря, составление технических регламентов с ошибками (отсутствие разделов), модификация тех-

нических регламентов, а также отсутствие реального тестирования регламентов для обеспечения основного бизнес-процесса ведет к риску остановки непрерывности бизнеса.

Следует отметить, что реализация вышеуказанных угроз также воздействует на программно-аппаратные комплексы обеспечения технологического процесса предприятия и может привести к выходу их из строя. Также основными угрозами на программно-аппаратные комплексы являются наличие вредоносного программного обеспечения и неквалифицированный персонал. Реализация вышеуказанных угроз ведет к риску остановки непрерывности бизнеса.

Для оценки вероятности реализации угрозы используется следующая шкала (табл. 3).

Таблица 3

Возможные значения вероятности реализации угрозы

Вероятность	Описание
Высокая	Есть вероятность возникновения одной или нескольких реализаций угрозы в пределах года
Средняя	Есть вероятность реализации угрозы в пределах двух-трех лет
Низкая	Возникновение влияния в пределах трех лет маловероятно

Для того, чтобы сопоставить все риски организации, определяем ущерб от реализации конкретной угрозы согласно табл. 4.

Таблица 4

Возможные значения ущерба от реализации угрозы

Ущерб	Описание
Высокий	Серьезные повреждения или полный выход актива из строя
Средний	Средние повреждения или ущерб
Низкий	Незначительные повреждения или ущерб

Природа рисков такова, что одно и то же рисковое событие может порождать разные по видам и величине ущербы. Ущербы характеризуются неопределенностью и зависимостью от факторов, определяющих состояние процесса целенаправленной деятельности [5, с. 129].

Можно указать на практически полную аналогию величины возникающего ущерба с рисковыми событиями с точки зрения его возникновения, анализа и оценки. Однако ущерб рассматривается как условная сущность, а влияние выделенных факторов величины ущерба рассматривается на практике с учетом естественной способности процесса противостоять рисковым событиям. Необходимо учитывать ущерб, который понесет не только актив, но и связанные активы. Ведь при нарушении целостности одного актива может пострадать все производство.

Реестр информационных рисков – основной документ, описывающий текущую ситуацию с рисками в организации [6, с. 7]. Приведем пример формирования реестра рисков для организации, имеющей 3 уровня управления. Для уровня «Актив» ранг реализации угрозы определяется согласно матрице определения ранга угрозы активу (РУА), составляется реестр рисков для каждого актива (табл. 5).

Таблица 5

Возможные значения ранга угрозы активу

Ущерб, причинённый активу в случае успешной реализации угрозы	Вероятность возникновения угрозы активу		
	Высокая	Средняя	Низкая
Высокий	1	3	6
Средний	2	7	9
Низкий	6	11	13

Ранг безопасности актива (РБА) определяется как минимальное значение РУА среди всех угроз, которым подвержен актив.

РБА формируется для определения уровня подверженности актива угрозам для данного бизнес-процесса, а также для дальнейшего формирования реестра рисков на остальных уровнях (табл. 6).

Таблица 6

Уровень подверженности актива угрозам

Уровень	РБА	Описание
Критический	1...4	Связанные с риском действия должны быть выполнены немедленно и в обязательном порядке
Средний	5...8	Связанные с риском действия должны быть предприняты в ближайшее время. Требуется мониторинг ситуации
Низкий	9...15	Никаких действий в данный момент предпринимать не требуется

Матрица определения ранга угрозы бизнес-процессу (РУБП) и уровня подверженности бизнес-процесса угрозам представлена в табл. 7.

Таблица 7

Возможные значения ранга угрозы бизнес-процессу

Важность актива	РБА														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Важные	1	2	3	4	5	6	13	14	15	16	17	18	49	50	51
Средней важности	7	8	9	10	11	12	19	20	21	22	23	24	52	53	54
Маловажные	25	26	27	28	29	30	31	32	33	34	35	36	55	56	57

На данном этапе производятся такие же действия, как и в предыдущем этапе, только для бизнес-процессов. Ранг безопасности бизнес-процесса (РББП) определяется как минимальное значение РУБП среди всех угроз, которым подвержен бизнес-процесс (табл. 8).

Таблица 8

Уровень подверженности бизнес-процесса угрозам

Уровень	РББП	Описание
Высокий	1...19	Связанные с риском действия должны быть выполнены немедленно и в обязательном порядке
Средний	20…38	Связанные с риском действия должны быть предприняты в ближайшее время, а также должен проводиться мониторинг
Низкий	39...57	Никаких действий в данный момент предпринимать не требуется

Для последующих уровней формируется реестр на основе рангов угроз. Ранг угроз уровня (РУУ) определяется как сумма РУБП и корректирующей переменной. Таблица возможных значений корректирующей переменной представлена в табл. 9.

Таблица 9

Таблица возможных значений корректирующей переменной

Уровень важности бизнес-процесса	Уровень подверженности бизнес-процесса угрозам		
	Высокий	Средний	Низкий
Важный	0	18	48
Средней важности	54	54	87
Мало-важный	89	92	92

Ранг безопасности организации (РБО) определяется как минимальное значение РУУ среди всех угроз последнего уровня детализации. Уровень подверженности организации угрозам определяется согласно табл. 10 и демонстрирует общее состояние защищенности организации.

Таблица 10

Уровень подверженности организации угрозам

Уровень	РБО	Описание
Критический	1...18	Связанные с риском действия должны быть выполнены немедленно и в обязательном порядке
Высокий	19…54	Связанные с риском действия должны быть предприняты в ближайшее время
Средний	55...105	Связанные с риском действия должны быть предприняты

В реестре записываются все реализации возможных угроз и расставляются в соответствии с рангом.

В зависимости от величины ущерба и определяется критичность угрозы. Поэтому вопрос распределения ответственности очень важен. Назначение владельцев исследуемых объектов организации позволяет упростить систему ранжирования рисков без потери качества, с увеличением последнего, благодаря применению механизмов ответственности.

Рассмотренные выше факторы в совокупности формируют ранжированный реестр рисков и образуют систему причинно-следственных отношений. Понимание всех взаимодействий системы приведет к получению системы управления информационными рисками, максимально подходящей для организации, в соответствии с требованиями стандартов информационной безопасности [7, с. 56]. Данная методика также позволяет рассчитывать риск с учетом человеческого фактора. В соответствии с многоуровневой картой бизнес-процессов создается реестр ресурсов и должностей сотрудников в соответствии с важностью и критичностью ресурса и уровнем компетентности человека. Для каждой должности описываются минимальные требования к сотруднику, претендующему на данную вакансию, в соответствии с его психофизиологическими ресурсами, уровнем образования и соответствующим опытом работы. В данном случае компетентность считается высокой и соответствует важности и критичности обслуживаемого ресурса. В противном случае компетентность считается низкой, что влечет за собой высокий уровень вероятности реализации угрозы относительно соответствующего актива. При оценке риска обязательно рассматриваются такие факторы, как психофизиологические свойства человека, соответствующие данному виду деятельности, образование, профессиональный опыт, что соответствует высокому уровню компетентности и, как следствие, мотивации к данному виду деятельности. Для каждого сотрудника составляется ранжированная, в зависимости от критичности актива, психолого-компетентностная карта бизнес-процессов организации. Сравнивая критичность актива и ожидаемые результаты предстоящей деятельности в соответствии с компетентностями сотрудника, можно определить наиболее уязвимые места с точки зрения человеческого фактора. Данная методика позволяет определить уровень вероятности инсайдерских атак.

Таким образом, благодаря применению несложных механизмов анализа создана методика оценки информационных рисков, соответствующая требованиям международных и российских стандартов, требованиям федерального закона 152 ФЗ о защите персональных данных. Простота технологии при распределении функциональных обязанностей в соответствии с активом позволяет значительно сократить временные показатели, финансовые и материальные средства для внедрения данной методики, что является одним из важных условий в рамках решаемой проблемы. Описание механизма учета человеческого фактора является несомненным преимуществом перед большинством из существующих методов.

Внедрение данной методики в торгово-ориентированном предприятии позволило сократить временные показатели для ведения основного бизнес-процесса предприятия, а также оптимизировать вспомогательные бизнес-процессы, что позволило предприятию существенно сократить финансовые и материальные затраты.

Библиографические ссылки

1. Ступина А. А., Золотарев А. В. Сравнительный анализ методов решения задачи оценки защищенности автоматизированных систем // Вестник СибГАУ. 2012. Вып. 4(44). С. 56–60.

2. Антамошкин О. А., Пузанова Г. А., Онтужев В. В. Особенности проектирования автоматизированной системы экспертной оценки информационной безопасности организаций // Вестник СибГАУ. 2013. Вып. 3(49). С. 4–9.

3 Репин В. Бизнес-процессы. Моделирование, внедрение, управление. М. : Манн, Иванов и Фербер, 2013. 512 с.

4. Балдин К. В. Риск-менеджмент : учеб. пособие. М. : Эксмо, 2006. 368 с.

5. Обеспечение информационной безопасности бизнеса / Андрианов В. В. [и др.] ; под ред. А. П. Курило. М. : Альпина Паблишер, 2011. 392 с.

6. Бондарь И. В. Методика построения модели угроз безопасности информации для автоматизированных систем // Вестник СибГАУ. 2012. Вып. 3(43). С. 7–10.

7. Астахов А. М. Искусство управления информационными рисками. М. : ДМК Пресс, 2010. 312 с.

References

1. Stupina A. A., Zolotarev A. V. [Comparative analysis of methods for solving the problem of security assessment STI-automated systems]. *Vestnik SibGAU*, 2013, vol. 44, no. 4, p. 56–60. (In Russ.)

2. Antamoshkin O. A., Puzanova G. A., Ontuzhev V. V. [Features of designing an automated peer review system information security organizations]. *Vestnik SibGAU*, 2013, vol. 49, no. 3, p. 4–9. (In Russ.)

3. Repin V. *Biznes-protsessy. Modelirovaniye, vnedreniye, upravleniye* [Business Processes. Modeling, implementation, management]. Moscow, Mann, Ivanov and Ferber Pudl., 2013, 512 p.

4. Baldin K. V. *Risk-menedzhment* [Risk management]. Moscow, Eksmo Publ., 2006, 368 p.

5. Andrianov V. V., Marshmallows S. L., Golovanov V. B., Golduev N. A., Kurylo A. P. *Obespecheniye informatsionnoy bezopasnosti biznesa* [Providing business information security]. Moscow, Alpina Publ., 2011, 392 p.

6. Bondar I. V. [The method of constructing models of information security threats for automated systems]. *Vestnik SibGAU*, 2012, vol. 43, no. 3, p. 7–10. (In Russ.)

7. Astakhov A. M. *Iskusstvo upravleniya informatsionnymi riskami* [The art of managing information risk]. Moscow, DMK Press Publ., 2010, 312 p.

УДК 004.9

К ВОПРОСУ ОБ УПОРЯДОЧЕНИИ МНОГОУРОВНЕВОЙ СЕМАНТИЧЕСКОЙ СЕТИ НА ДЕРЕВЕ СЕМАНТИЧЕСКОЙ КЛАССИФИКАЦИИ

Д. В. Личаргин[1], К. В. Сафонов[2], О. И. Егорушкин[2], Е. П. Бачурина[1]

[1]Сибирский федеральный университет
Российская Федерация, 660074, г. Красноярск, ул. Академика Киренского, 26
[2]Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Российская Федерация, 660014, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: lichdv@hotmail.ru

Рассматривается проблема представления глубинной семантики слов, предложений, повествований и текстов на естественном языке в рамках такой формы представления данных, как семантические сети. Предлагается модель многоуровневой семантической сети слов, в которой узлы и дуги графа слов включают графы вложенных в неё семантических сетей сем. Предложен способ представления соответствий между уровнями семантической сети на уровне слов и на уровне сем на основе матриц, содержащих тождественные аргументы элементов значений слов естественного языка. Затрагивается вопрос об упорядочении многоуровневой семантической сети на векторизованной семантической классификации данных. Делается вывод о необходимости продолжения данного исследования с учетом необходимости разработки программы для генерации матриц описания глубинной семантики слов.

Ключевые слова: многоуровневые семантические сети, компьютерная лингвистика, семантическая классификация, представление данных.