Оценка устойчивости развития критической инфраструктуры Российской Федерации на базе технологии оценки и мониторинга информационной безопасности

Михалевич И.Ф, Рыжов А.П.

В работе рассмотрены возможности применения технологии оценки и мониторинга сложных процессов обеспечения информационной безопасности в задаче устойчивого развития критической инфраструктуры Российской Федерации. Предложена структура модели устойчивости критической инфраструктуры, возможные сценарии использования системы оценки и мониторинга информационной безопасности, обсуждаются аналитические возможности системы.

Ключевые слова: информационная безопасность, критическая инфраструктура, технология оценки и мониторинга сложных процессов, устойчивое развитие.

1. Введение.

Концепция устойчивого развития во многом перекликается с концепцией ноосферы, выдвинутой академиком В. И. Вернадским ещё в середине XX века. Ее современное толкование берет начало с 70-х годов прошлого столетия, когда человечество столкнулось с вопросами ограниченности природных ресурсов, а также загрязнения природной среды, которая является основой жизни, экономической и любой деятельности человека. Реакцией на эту озабоченность было создание международных неправительственных научных организаций по изучению глобальных процессов на Земле, таких как Международная федерация институтов перспективных исследований (ИФИАС), Римский клуб (с его знаменитым докладом «Пределы роста»), Международный институт системного анализа, а в СССР — Всесоюзный институт системных исследова-

ний. Проведение в 1972 году в Стокгольме Конференции ООН по окружающей человека среде и создание Программы ООН по окружающей среде (ЮНЕП) ознаменовало включение международного сообщества на государственном уровне в решение экологических проблем, которые стали сдерживать социально-экономическое развитие. Всемирная стратегия охраны природы (ВСОП), принятая в 1980, впервые в международном документе содержала упоминание устойчивого развития. Вторая редакция ВСОП получила название «Забота о планете Земля — Стратегия устойчивой жизни» и была опубликована в октябре 1991. В ней подчеркивается, что развитие должно базироваться на сохранении живой природы, защите структуры, функций и разнообразия природных систем Земли, от которых зависят биологические виды. Для этого необходимо: сохранять системы поддержки жизни (жизнеобеспечения), сохранять биоразнообразие и обеспечить устойчивое использование возобновляемых ресурсов. Появились исследования по экологической безопасности как части национальной и глобальной безопасности.

Частью национальной и глобальной безопасности современного мира является информационная безопасность [1 – 4]. Нарушения безопасности информации, такие как несанкционированное раскрытие или изменение информации, блокирование доступа к информации способны существенно воспрепятствовать любому росту, особенно, если это касается критических инфраструктур. В связи с этим вопросы оценки и мониторинга информационной безопасности стоят в ряду приоритетных задач обеспечения устойчивого развития критических инфраструктур [5 – 12].

С технической точки зрения вопросы устойчивости изучались в рамках кибернетики. Наиболее близким понятием является понятие гомеостаза. Возникли специальные математические модели экономического развития, учитывающие устойчивость развития (например, модель Солоу-Свана, гравитационная модель, Модель Рамсея-Касса-Купманса, Модель пересекающихся поколений или модель Самуэльсона-Даймонда). Обсуждению данной проблематики также уделяется внимание в русскоязычной литературе (например, [13], [16]; библиография [17]), выпускаются специальные журналы [14], консалтинговые компании предлагают услуги в области устойчивого развития [15].

Систематическая работа с оценкой и мониторингом устойчивого развития предполагает создание специальной системы. Одним из авторов работы разработана технология оценки и мониторинга сложных процессов [18], которая была успешно использована для разработки систем оценки и мониторинга способности стран к производству специальных

технологий в ядерной области в интересах управления международных гарантий Международного Агентства по Атомной Энергии [19], оценки и мониторинга способности команды разработчиков микроэлектроники к выполнению проекта для компании Cadence Design Systems [20], оценки и мониторинга рисков атеросклеротических заболеваний [21] и других систем.

В настоящей работе представлено видение авторов по возможному решению задачи устойчивого развития критической инфраструктуры Российской Федерации на базе технологии оценки и мониторинга сложных процессов применительно к обеспечению информационно безопасности.

Информационная безопасность критической инфраструктуры

Критическую инфраструктуру стран образуют системы и активы, нарушение функционирования или уничтожение которых оказывает деструктивное влияние на жизненно важные для них сферы. Так, в критической инфраструктуре РФ можно выделить следующие сектора и области: здравоохранение, наука, транспорт, связь, энергетика, банковская и иные сферы финансового рынка, топливно-энергетический комплекс, атомная энергетика, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность, химическая промышленность, федеральные органы государственной власти, органы государственной власти субъектов РФ, органы местного самоуправления, российские юридические лица и индивидуальные предприниматели, которые обеспечивают функционирование и взаимодействие элементов критической инфраструктуры РФ [1 – 5].

Деятельность критических инфраструктур невозможна без информационного взаимодействия, что делает устойчивость их развития зависимой от информационной безопасности [11, 12]. В каждой критической инфраструктуре образуется критическая информационная инфраструктура (КИИ), включающая свои объекты и телекоммуникации, используемые для организации взаимодействия объектов. Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» безопасность КИИ РФ определена как состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Значимость объектов КИИ определяется возможным ущербом, причиняемым жизненно важным интересам (процессам) при нарушении их

функционирования. Вышеназванным законом к критериям значимости объектов КИИ РФ отнесены социальная, политическая, экономическая, экологическая важность, важность для обеспечения обороны страны, безопасности государства и правопорядка, которые основаны на соответствующих оценках $[3-5]$:

социальная - в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к системам обеспечения правосудия, правопорядка, государственным и муниципальным услугам и т.п. для получателей таких услуг;

политическая - в оценке возможного причинения ущерба интересам страны в вопросах внутренней и внешней политики;

экономическая - в оценке возможного причинения прямого и/или косвенного ущерба субъектам экономической деятельности;

экологическая - в оценке уровня возможного ущерба окружающей среде;

и т.д.

Таким образом, оценка и мониторинг информационной безопасности КИИ РФ и критической инфраструктуры в целом являются существенными факторами устойчивости их развития [1, 2].

Технология оценки и мониторинга: особенности разработки приложений

Технология оценки и мониторинга сложных процессов ориентирована на разработку человеко-компьютерных систем для оценки состояния и отслеживания развития процессов в бизнесе, экономике, социологии, политике и других областях, которые принято называть слабо или плохо формализуемыми. Для таких процессов почти всегда невозможно построить математическую модель в привычном понимании (в виде уравнений, автоматов и пр.) либо модель является очень абстрактной и ее практическое использование невозможно. Трудности связаны не только со сложностью самих процессов, но и с неизмеримостью значений их параметров в привычном виде чисел; «измерительным прибором» для таких параметров является человек. Однако, есть аналитики, решающие задачу оценки и мониторинга на систематической основе, поэтому автоматизация их работы является осмысленной задачей. Разработка таких систем возможна, когда можно построить семантическую модель про-

цесса в виде набора понятий и их взаимосвязей, а также поступает и анализируется реальная информация - возможны обучение и настройка. Схема работы систем оценки и мониторинга представлена на рис. 1.

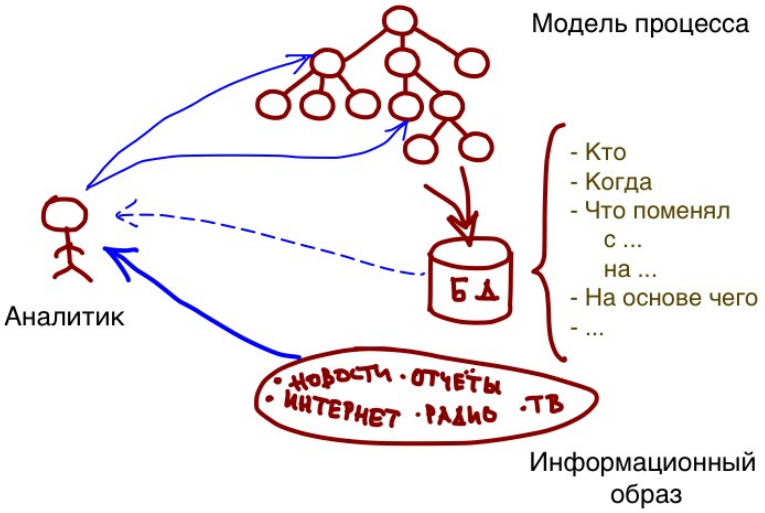

Рис. 1. Схема работы систем оценки и мониторинга.

При практической реализации систем оценки и мониторинга возникают следующие проблемы.

Проблема 1 (описание человеком объектов). Можно ли, учитывая некоторые особенности восприятия человеком объектов реального мира и их описания, сформулировать правило выбора оптимального множества значений признаков, по которым описываются эти объекты? Возможны два критерия оптимальности:

Критерий 1. Под оптимальными понимаются такие множества значений, используя которые человек испытывает минимальную неопределенность при описании объектов.

Критерий 2. Если объект описывается некоторым количеством экспертов, то под оптимальными понимаются такие множества значений, которые обеспечивают минимальную степень рассогласования описаний.

Показано, что мы можем сформулировать методику выбора оптимального множества значений качественных признаков. Более того, показано, что такая методика является устойчивой, то есть возможные при

построении функций принадлежности естественные маленькие ошибки не оказывают существенного влияния на выбор оптимального множества значений. Множества, оптимальные по критериям 1 и 2 совпадают.

Проблема 2 (поиск информации, описанной человеком). Можно ли определить показатели качества поиска информации в нечетких (лингвистических) базах данных и сформулировать правило выбора такого множества лингвистических значений, использование которого обеспечивало бы максимальные показатели качества поиска информации?

Показано, что можно ввести показатели качества поиска информации в нечетких (лингвистических) базах данных и формализовать их. Показано, что возможно сформулировать методику выбора оптимального множества значений качественных признаков, которое обеспечивает максимальные показатели качества поиска информации. Более того, показано, что такая методика является устойчивой, то есть возможные при построении функций принадлежности естественные маленькие ошибки не оказывают существенного влияния на выбор оптимального множества значений.

Проблема 3 (агрегирование информации). Можно ли предложить алгоритмы выбора операторов агрегирования информации в системах информационного мониторинга, обеспечивающие «настройку» системы на конкретную предметную область?

Выделяются следующие подходы к решению этой проблемы, базирующиеся на различных интерпретациях операторов агрегирования информации: геометрический, логический, и на основе обучения. Последний включает в себя обучение на основе генетических алгоритмов и обучение на основе нейронных сетей.

Перечисленные выше результаты решения проблем 1- 3 подробно описаны в [18]. Они позволяют разрабатывать оптимальные с точки зрения удобства использования системы оценки и мониторинга сложных процессов.

Таким образом, основной задачей разработки приложения является построение модели процесса.

Модель процесса устойчивого развития

Модель процесса состоит из двух частей: структуры и правил агрегирования информации. Структура представляет собой дерево или граф без циклов, вершины которого представляют собой понятия предметной области, ребра – связи между ними. Пример структуры процесса оценки

и мониторинга информационной безопасности КИИ РФ приведен на рис. 2.

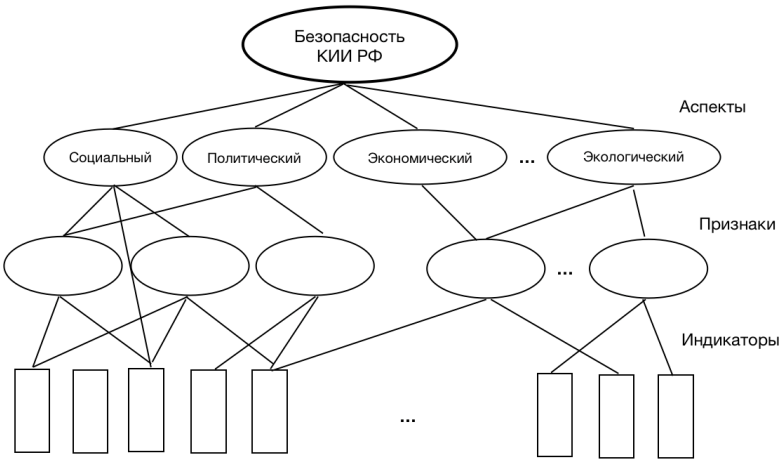

Рис. 2. Пример структуры модели

Логика работы модели задается операторами агрегирования информации, вычисляющими оценки узлов верхнего уровня в зависимости от значений оценок подчиненных узлов. Настройка модели для конкретной задачи заключается в обучении операторов агрегирования информации. Классификация операторов агрегирования информации, условия их применимости, а также эти процедуры обучения детально описаны в [22].

На верхнем уровне факторы устойчивого развития можно разделить на внешние и внутренние. Факторы внешней среды оказывают прямое или косвенное влияние на деятельность предприятия и действуют за ее пределами. Поэтому для обеспечения устойчивости своего функционирования компании должны оперативно реагировать на изменения внешней среды (законодательство, состояние и тренды рынка, требования инвесторов и пр.) и принимать эффективные решения. Факторы внутренней среды (организационная структура компании, эффективность производственных процессов, состав и квалификация персонала, организация труда и методы управления, состояние материально-технической базы и технологии) оказывают значительное влияние на устойчивость развития предприятия и являются более контролируемыми.

Заметим, что часто такая модель используется в достаточно зрелых бизнес-структурах – это сбалансированная система показателей (Balanced ScoreCard). Если одной из стратегических целей организации

является устойчивое развитие – то соответствующая часть сбалансированной системы показателей может являться моделью для системы оценки и мониторинга. В противном случае модель строится на тех же принципах и с использованием тех же механизмов, что и сбалансированная система показателей.

Возможные сценарии использование системы оценки и мониторинга в задаче оценки устойчивого развития критических инфраструктур

Заметим, что различные аспекты системы оценки и мониторинга устойчивого развития так или иначе присутствуют в любой организации, обеспечивающей деятельность объектов КИИ РФ и критической инфраструктуры РФ, и являются зоной ответственности различных подразделений. Например, оценку и мониторинг информационной безопасности в организации осуществляет служба безопасности (СБ), факторов внешней среды - СБ, ИТ, PR/GR, юридическая служба, маркетинг, факторов внутренней среды – СБ, ИТ, HR, производственные подразделения. Внедрение системы оценки и мониторинга устойчивого развития позволит иметь целостную картину этой работы в КИИ РФ и критической инфраструктуре РФ в целом. Такой эффект достигается благодаря тому, что модель (благодаря ее структуре – дерево или граф без циклов) можно «разрезать» на ряд подмоделей. Каждая служба компании может работать со своим фрагментом модели (что она и так делает, только такая работа будет более прозрачной, измеримой, дающей возможности решения дополнительных аналитических задач), а руководство компании будет иметь целостную картину состояния устойчивости компании (рис. 3).

В рамках систем оценки и мониторинга возможно решение прямой и обратной задачи оценки информационной безопасности и устойчивости КИИ РФ и критической инфраструктуры РФ.

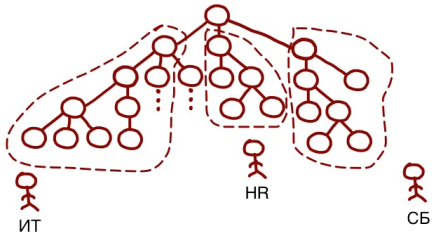

Рис. 3. Возможности декомпозиции систем оценки и мониторинга.

Прямая задача заключается в нахождении критических путей – таких элементов модели, малое изменение которых приводит к изменению всех вышележащих узлов, включая верхний. Знание таких элементов имеет большое практическое значение и позволяет выявить "слабые места"в процессе на текущий момент времени, разработать мероприятия по блокированию нежелательных ситуаций или провоцированию желательных, т.е. управлять развитием процесса в интересах компании. Для большого класса операторов агрегирования информации возможно вычисление степени критичности каждого элемента модели [22]. Задача также может решаться перебором для достаточно компактной модели.

Обратная задача позволяет оптимизировать бюджет на достижение определённого уровня устойчивости. Если задан бюджет, и мы знаем стоимость изменения состояния узла модели, то возможно нахождение тех узлов, изменение которых находится в рамках заданного бюджета и дает максимальной эффект повышения устойчивости компании. При заданных условиях возможно и решение сопряжённой задачи: нахождение минимального бюджета, позволяющего достичь необходимый уровень устойчивости.

Перечисленные задачи можно решать как в рамках фрагментов модели (оптимизация работы соответствующих объектов КИИ РФ), так и модели в целом (оптимизация КИИ РФ по повышению устойчивости критической инфраструктуры РФ).

Список литературы

[1] Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646.

[2] Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы. Утверждена Указом Президента Российской Федерации от 09.05.2017 г. № 203.

[3] Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[4] Critical Infrastructure Threat Information Sharing Framework. A Reference Guide for the Critical Infrastructure Community. USA Homeland Security, October 2016. – 110 p.

[5] Правила категорирования объектов критической информационной инфраструктуры Российской Федерации. Утверждены постановлением Правительства Российской Федерации от 08.02.2018 г. № 127.

[6] Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения. Утвержден постановлением Правительства Российской Федерации от 08.02.2018 г. № 127.
[7] Critical Information Infrastructures Protection approaches in EU. Final Document | Version 1 | TLP: Green | July 2015. – 19 p. -
https://resilience.enisa.europa.eu/enisas-ncss-project/
CIIPApproachesNCSS.pdf.
[8] Matt Barrett, Jeff Marron, Victoria Yan Pillitteri, Jon Boyens, Greg Witte, Larry Feldman. The Cybersecurity Framework. Implementation Guidance for Federal Agencies. Draft Report 8170. U.S. Department of Commerce. National Institute of Standards and Technology Interagency. - May 2017. - 41 p. - https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf.
[9] Don Snyder, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, Michael H. Powell. Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles. – 74 p. -
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf.
[10] A Generic National Framework For Critical Information Infrastructure Protection (CIIP). ITU, 2007. - 30 p. -
www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf.
[11] Михалевич И.Ф. Концепция создания доверенной среды функционирования автоматизированных систем в защищенном исполнении на базе операционной системы «Синтез-ОС». – М.: ООО «АйТиСириус», 2012. – 50 с. [Электронный ресурс]. URL: https://www.itsirius.su/resheniya/ (дата обращения: 20.12.2012).
[12] Михалевич И.Ф. Проблемы создания доверенной среды функционирования автоматизированных систем управления в защищенном исполнении / Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). - М.: Институт проблем управления им. В.А.Трапезникова РАН, 2014. - С. 9201-9207.
[13] Критерии устойчивости предпринимательской деятельности в условиях мировой экономической рецессии / Российское предпринимательство № 1, вып. 2 (176), 2011. - С. 57-61
[14] Устойчивый бизнес. Экспертный деловой журнал.
http://csrjournal.com/
[15] Обзор услуг в области чистых технологий и устойчивого раз-

вития. Ernst & Young - http://www.ey.com/RU/ru/Services/Specialty-Services/Climate-Change-and-Sustainability-Services.
[16] Корчагина Е.В. Сравнительный анализ отчетности устойчивого развития российских и зарубежных компаний / Проблемы современной экономики. № 4 (28), 2008.
[17] http://www.m-economy.ru/keyword.php?id=3209&l=R
[18] Рыжов А.П. Информационный мониторинг сложных процессов: технологические и математические основы / Интеллектуальные системы, т. 11, вып. 1-4, 2008. - С. 101-136.
[19] Ryjov A., Belenki A., Hooper R., Pouchkarev V., Fattah A., Zadeh L. A. Development of an Intelligent System for Monitoring and Evaluation of Peaceful Nuclear Activities (DISNA). IAEA, STR-310. Vienna, 1998, 122 p.
[20] Лебедев А.А., Рыжов А.П. Оценка и мониторинг проектов разработки высокотехнологичных изделий на примере микроэлектроники / Интеллектуальные системы, т. 11, вып. 1-4, 2008. С. 55-82.
[21] Ахмеджанов Н.М., Жукоцкий А.В., Кудрявцев В.Б., Оганов Р.Г., Расторгуев В.В., Рыжов А.П., Строгалов А.С. Информационный мониторинг в задаче прогнозирования риска развития сердечно-сосудистых заболеваний / Интеллектуальные системы, т. 7, вып. 1-4, 2003. С. 5 – 38.
[22] Рыжов А.П. Об агрегировании информации в нечетких иерархических системах / Интеллектуальные системы, т. 6, вып. 1-4, 2001. - С. 341.

Assessment of the sustainability of the development of the critical infrastructure of the Russian Federation on the basis of information security assessment and monitoring technology

Igor F. Mikhalevich, Alexandr P. Ryjov

The paper considers the possibilities of applying the technology of assessment and monitoring of complex processes of ensuring information security in the task of sustainable development of the critical infrastructure of the Russian Federation. The structure of the critical infrastructure stability model, the possible scenarios for the system of information security assessment and monitoring, the analytical capabilities of the system are discussed.

Keywords: information security, critical infrastructure, technology for assessment and monitoring of complex processes, sustainable development.