ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.891.3

ПРИМЕНЕНИЕ ЭКСПЕРТНЫХ СИСТЕМ С УЧЕТОМ ОТРАСЛЕВОЙ СОСТАВЛЯЮЩЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Киреева Н.В., Поздняк И.С., Филиппов Н.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: kireeva@psuti.ru

В статье рассмотрена задача исследования параметров комплексной оценки информационной безопасности организации. Предложено формирование информационной основы экспертной системы на основе государственных стандартов в области информационной безопасности и различных отраслевых требований. С основой на стандарты предложены способы наполнения базы данных экспертной системы и модель функционирования данной системы. Указаны особенности наполнения информационной базы экспертной системы при использовании отраслевых требований, которые должны учитывать возможность наличия в базе неких вопросов и знаний, что определяет необходимость тщательной проверки наполнения базы данных этой системы для конкретной отрасли. Используя алгоритм взаимодействия пользователя с механизмом вывода, в процессе оценки информационной безопасности возможно выделить отраслевую составляющую, что позволяет более точно определить риски и выработать рекомендации по защите информационной системы. Кроме того, предлагается способ взаимодействия компонентов механизма логического вывода.

Ключевые слова: *информационная база, экспертная система, отраслевая составляющая, стандарты, риски, информационная безопасность*

Введение

В настоящее время любая организация занимается хранением или обработкой информации. Важной составляющей контроля за состоянием информационной безопасности (ИБ) при этом является аудит, который заключается в получении объективных качественных и количественных оценок о текущем состоянии ИБ организации в соответствии с принятыми критериями и показателями безопасности. Аудит требует от проверяющего глубокого знания законодательной базы в области защиты информации, а также учета специфики хранимых и обрабатываемых данных в информационной системе, принадлежащей организации.

Экспертные системы (ЭС) разрабатываются с целью облегчить и автоматизировать деятельность экспертов в той или иной области. Цель работы – создание ЭС, в рамках которой возможно проводить комплексную оценку ИБ как для типовой информационной системы, так и для конкретных систем предприятий газовой, энергетической, телекоммуникационной и т. д. отрасли [1]. При этом предполагается разработать алгоритм взаимодействия пользователя и информационной системы, который позволит при необходимости выделить отраслевую составляющую в процессе оценки ИБ, а также подробно описать методику наполнения внутренней базы данных ЭС.

Состав и структура ЭС

Существующие системы аудита могут быть основаны на ЭС, которые сегодня используются в различных областях для оценки рисков. Важной их особенностью является способность к самообучению, которая связана с непрерывным процессом обнаружения знаний и интеллектуальным анализом данных. По мнению специалистов, в недалеком будущем ЭС будут играть ведущую роль во всех фазах проектирования, разработки, производства, распределения, продажи, поддержки и оказания услуг [2]. Их технология, получив коммерческое распространение, обеспечит революционный прорыв в интеграции приложений из готовых интеллектуально взаимодействующих модулей. Однако при описании предметной области ЭС часто остаются неизвестными и неоцененными отраслевые составляющие, что обуславливает актуальность и практическую значимость изучения задачи, решаемой в данной статье.

Современные ЭС в большинстве своем очень узконаправлены и не всегда дают желаемый эффект. Схема функционирования ЭС в общем виде представлена на рисунке 1.

Ключевыми элементами ЭС являются база данных, база знаний и аппарат логического вывода. При этом ЭС должна позволять строить структурные модели информационной системы, моде-

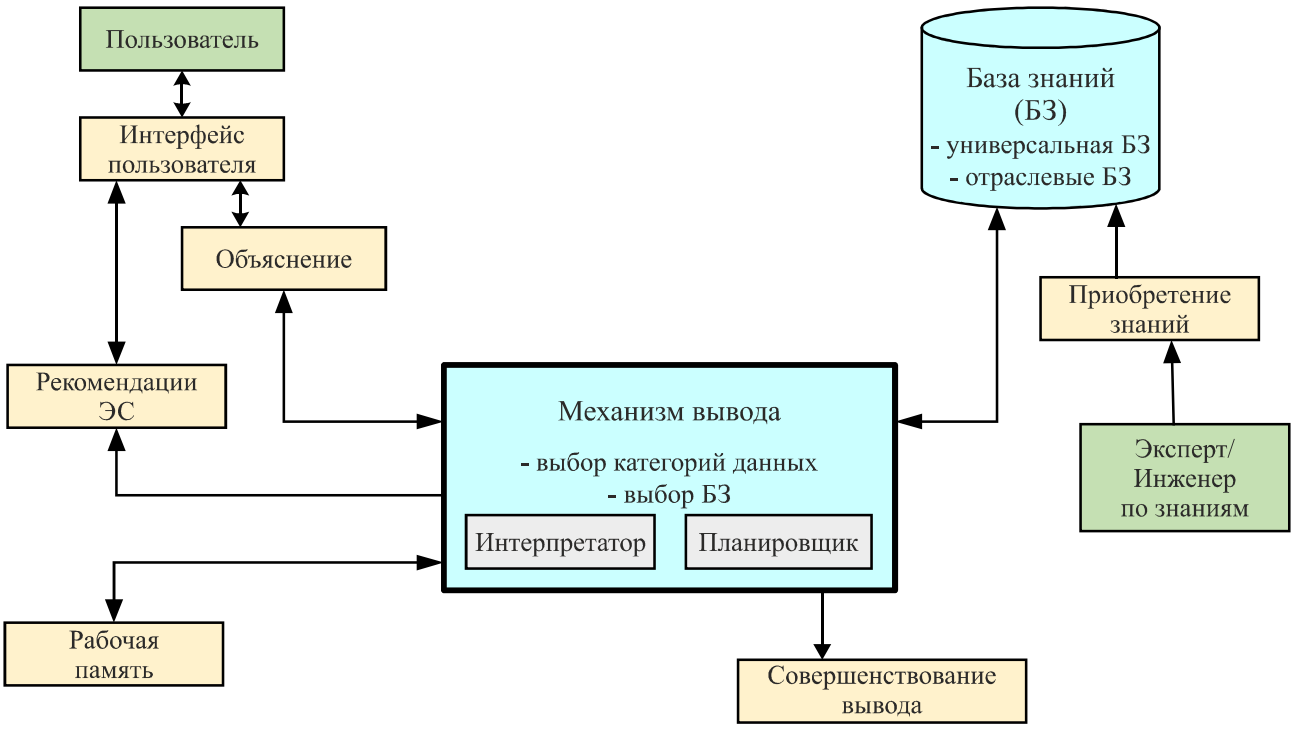

Рисунок 1. Взаимодействие элементов ЭС

ли угроз и уязвимостей, связанные с отдельными составляющими информационной системы. Это позволит выявить те элементы и объекты информационной системы, риск и ущерб от нарушения ИБ которых является наиболее критичным. При построении ЭС наиболее трудоемким является процесс приобретения необходимых знаний, в ходе которого инженер по знаниям решает, какой метод инженерии знаний будет использоваться и каким образом он будет взаимодействовать с экспертом (наблюдательный это или интуитивный подход) [3]

Используя одну или несколько стратегий получения знаний (приобретение, извлечение и формирование), необходимо получить вербальное описание предметной области задачи. Основой для описания служат цели, подцели, результирующая и исходная управленческая документация, а также опыт эксперта и специальная литература [4]. В нашей работе базу данных ЭС будем строить на основе стандартов в области информационной безопасности и различных отраслевых документов (ГОСТ, ОСТ, РД, Технические требования, рекомендации отрасли). В дополнение к этому инженер по знаниям подготовит ряд типовых задач для обсуждения с экспертом.

Предметная область

Рассмотрим стандарт ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [5]. Раздел 6.1 «Задачи, решаемые внутри организации» рассматривает вопросы управления информационной безопасностью в организации. Для создания ЭС воспользуемся подразделами 6.1.1…6.1.8, в каждом из которых есть вопросы, необходимые для рассмотрения. Вопросы раздела 6.2 «Аспекты взаимодействия со сторонними организациями» (затрагивает вопросы поддержки безопасности средств обработки информации организации и информационных активов при доступе третьих сторон) также будут рассмотрены при описании предметной области.

Применение раздела 7 «Менеджмент активов» помогает определить активы, в отношении которых будет осуществляться оценка ИБ, а также соответствующая защита выбранных активов организации. Не нужно упускать из виду и организационные меры, касающиеся действий персонала. Для этого следует применять раздел 8 «Безопасность, связанная с персоналом». Сюда относятся и учет вопросов безопасности в должностных обязанностях при найме персонала (п. 8.1.1), и обучение пользователей (п. 8.2.2), и вопросы, связанные с прекращением или сменой занятости сотрудников (п. 8.3).

Раздел 9 «Физическая безопасность и защита от воздействий окружающей среды» содержит необходимые сведения для разрабатываемой ЭС об охраняемых зонах, безопасности оборудования внутри этих зон, а также общие мероприятия

по управлению ИБ. Раздел 10 «Менеджмент коммуникаций и работ» поможет наполнить базу данных ЭС информацией об эксплуатационных процедурах и обязанностях персонала; менеджменте оказания услуг третьей стороной; планировании и приемке систем; защите от вредоносной и мобильной программы; резервировании и пр.

Раздел 11 «Управление доступом» позволит пополнить ЭС знаниями о требованиях бизнеса по управлению доступом; менеджменте доступа пользователей; управлении доступом к информации и прикладным программам и др. Вопросы, связанные с разделом 12 «Приобретение, разработка и эксплуатация информационных систем», разделом 13 «Менеджмент инцидентов информационной безопасности», разделом 14 «Менеджмент непрерывности бизнеса» и разделом 15 «Соответствие», также полностью будут рассмотрены при разработке ЭС. Более полно с этими разделами можно ознакомиться в [5].

Далее рассмотрим стандарт ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [6]. В Приложение А данного стандарта изложены цели и меры управления, которые тесно связаны с ГОСТ Р ИСО/МЭК 27002. Поэтому при наполнении базы данных разрабатываемой ЭС следует быть внимательным, чтобы не допустить повторения однотипных ситуаций. Например, раздел А.5 приложения соотносится с разделом 5 «Политика безопасности» (стандарт ИСО/МЭК 27002), раздел А.12 приложения – с разделом 12 «Приобретение, разработка и эксплуатация информационных систем» (стандарт ИСО/МЭК 27002). Исключение составляет раздел А.13 «Управление инцидентами информационной безопасности». Ему частично соответствует раздел 13.2 «Менеджмент инцидентов информационной безопасности и необходимое совершенствование» (стандарт ИСО/МЭК 27002).

Несмотря на это, цели и меры из Приложения А (стандарт ИСО/МЭК 27001) обязательны для включения в БЗ. В случае если они не перекрывают меры и способы управления ИБ (стандарта ИСО/МЭК 27002), то являются их дополнением. Перечень мер управления, содержащийся в эти двух стандартах, не является исчерпывающим и может быть дополнен инженером по знаниям и экспертом.

Следующий стандарт, на который следует обратить внимание при описании предметной области ЭС, – это ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». В базу следует внести типы активов (основные и вспомогательные), в отношении которых будут оцениваться риски [7].

Также в ЭС требуется понятие «ценность актива». При этом определять ее должны будут владельцы и пользователи активов в процессе использования ЭС. Кроме того, необходимо внести понятия «угроза», «источник угрозы», «объект угрозы», «вероятность реализации угрозы», «уязвимость», «степень уязвимости», «защитные меры». Перечень типичных видов угроз представлен в Приложении С стандарта, примеры общих уязвимостей приведены в Приложении D ГОСТ Р ИСО/МЭК 27005-2010.

Таким образом, в общей сложности три государственных стандарта в области ИБ легли в основу разрабатываемой ЭС. В них содержатся наиболее важные сведения (знания), отражающие комплексную оценку ИБ информационной системы любого предприятия. Помимо этого, необходимо рассмотреть и включить в ЭС данные различных отраслевых документов. Так как отраслей огромное количество, то включить все возможные стандарты и рекомендации не представляется возможным. Тем не менее наполнять базу данных следует с документов наиболее востребованных отраслей – например, банковского сектора. Для него существует ряд стандартов, которые помогут наполнить базу отраслевыми знаниями: СТО БР ИББС-1.0, СТО БР ИББС-1.1, СТО БР ИББС-1.2, РС БР ИББС-2.0, РС БР ИББС-2.2.

Одним из основных здесь является стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0). Раздел 7 этого документа позволяет определить требования по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу, требования по обеспечению ИБ автоматизированных банковских систем на стадиях жизненного цикла, а также требования по обеспечению ИБ при управлении доступом и регистрации, при использовании ресурсов сети Internet, при применении средств криптографической защиты информации, банковских платежных и информационных технологических процессов. Раздел 8 «Система менеджмента информационной безопасности организаций банковской системы Российской Федерации» подробно рассматривает вопросы

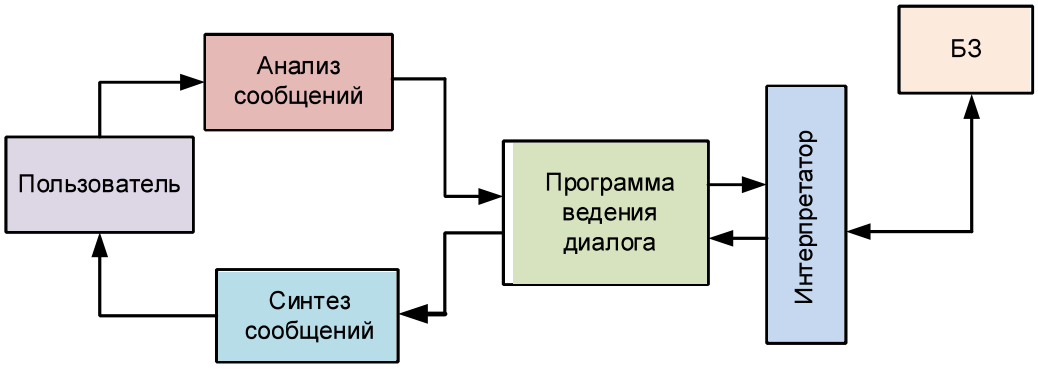

Рисунок 2. Взаимодействие компонентов МЛВ

управления ИБ, что позволит в полной мере наполнить базу данных и базу знаний ЭС информацией по банковской отрасли.

Большое внимание следует уделить вопросам безопасности автоматизированных систем управления технологическими процессами (АСУ ТП), так как большинство современных промышленных предприятий использует такие системы. Проблема обеспечения ИБ в АСУ ТП заключается в том, что специалисты в большинстве своем либо обладают знаниями в области только информационной безопасности, либо типичными знаниями АСУ ТП. Пересечений этих знаний крайне мало. В ЭС есть возможность объединить совокупность этих знаний, наполнив базу знаний на основе бесед с экспертами обоих типов [8].

Помимо этого, предполагается использовать ряд других стандартов, основными из которых являются части ГОСТ Р МЭК 62443: ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы; ГОСТ Р МЭК 62443-3-3-2016 Сети промышленной коммуникации. Безопасность сетей и систем.

Кроме того, для наполнения ЭС следует обратить внимание на стандарт NIST (National Institute of Standards and Technology) SP 800-82 Guide to Industrial Control Systems (ICS) Security. Во время заполнения ЭС с помощью отраслевых стандартов необходимо помнить, что ситуации, вопросы и знания уже могут быть внесены в базу. В этом случае следует проверять нюансы, связанные с конкретной отраслью.

Механизм логического вывода

Еще одним важным элементом ЭС (см. рисунок 2) является механизм логического вывода (МЛВ), необходимый для выявления новых фактов на основе сопоставления исходных данных из рабочей памяти (с помощью программы ведения диалога) и знаний из БЗ [9].

В структуре ЭС данный механизм задействует алгоритмы прямого и (или) обратного вывода и может быть представлен четверкой параметров {V, S, K, W} [10], где V – процедура выбора из базы знаний и рабочей памяти правил и фактов; S – процедура сопоставления правил и фактов, в результате которой определяется множество фактов, к которым применимы правила для присвоения значений; K – процедура разрешения конфликтов, определяющая порядок использования правил, если в заключение правила указаны одинаковые имена фактов с разными значениями; W – процедура, осуществляющая выполнение действий, соответствующих полученному значению факта (заключению правила).

Наполнение ЭС правилами осуществляется по ранее описанным методикам. Наполнение рабочей памяти фактами происходит в результате ввода требуемых сведений пользователем. Процедуры V и S тесно взаимосвязаны между собой и запускаются сразу после ввода фактов.

Результатом такого взаимодействия является процедура W. После выполнения определенных действий, заложенных в W, пользователю выдается требуемый результат в виде рекомендаций по защите выбранного актива и оценок. Отраслевая составляющая содержится в наборе правил и фактов. В случае если оценка ИБ требует ее наличия, пользователь должен уведомить об этом ЭС до ввода запрашиваемых фактов.

Заключение

Пользователь ЭС может не быть специалистом в данной отраслевой области, поэтому его взаимодействие с ЭС посредством МЛВ будет осуществляться при помощи алгоритма, позволяющего выделять составляющую для отрасли в процессе оценки ИБ. Пользователя при взаимодействии с ЭС интересует результат и (или) способ получения решения, его задача состоит в получении от ЭС решения ряда задач, а также ис-

пользовании системы для сокращения трудоемкости получения результата или повышения его качества.

В большинстве ЭС отсутствует простой и общий метод организации логического вывода. Его структура зависит и от специфики отраслевой области, и от того, как знания структурированы и организованы в ЭС. Поскольку МЛВ реализуют тот или иной способ рассуждения, технологию поиска по базе знаний, обработку неопределенности и обработку ошибок, ЭС могут иметь набор встроенных МЛВ, которые позволяют разработчику модифицировать или переопределять их для большего соответствия с отраслевой областью.

Наполнение базы знаний ЭС и построение МЛВ является значительной по объему и трудоемкой задачей. Предложенные особенности наполнения ЭС являются основой, вокруг которой в дальнейшем будет строиться система.

Литература

1. Созинова Е.Н. Применение экспертных систем для анализа и оценки информационной безопасности // Молодой ученый. 2011. Т. 1. № 10 (33). С. 61–66.
2. Бубнов Д.В. Экспертные системы как средство интеллектуальной поддержки технологических решений // Вестник МГТУ Станкин. 2011. № 4 (16). С. 83–86.
3. Джарратано Дж., Райли Г. Экспертные системы: принципы разработки и программирование / пер. с англ. М.: ИД «Вильямс», 2007. 1152 с.
4. Новые информационные технологии: подготовка кадров и обучение персонала. Часть 3. Интеллектуальные информационные системы и управление бизнес-процессами в инфокоммуникациях / Э.М. Димов [и др.]. Самара: Изд-во СамНЦ РАН, 2017. 440 с.
5. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М.: Стандартинформ, 2014. 106 с.
6. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2008. 31 с.
7. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М.: Стандартинформ, 2011. 51 с.
8. Андрианов В.И., Романов Г.Г., Штеренберг С.И. Экспертные системы в области информационной безопасности // IV МНТК и МНМК «Актуальные проблемы инфокоммуникаций в науке и образовании», АПИНО-2015: сб. тр. Санкт-Петербург, 2015. Т. 1. С. 193–197.
9. Коробулина О.Ю. База знаний экспертной системы аудита информационной безопасности // Программные продукты и системы. 2010. № 4. С. 89–91.
10. Структура экспертной системы. URL: http://www.aiportal.ru/articles/expert-systems/structure.html (дата обращения: 20.03.2019).

Получено 25.11.2019

Киреева Наталья Валерьевна, к.т.н., доцент, декан факультета телекоммуникаций и радиотехники Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 846 333-13-13. E-mail: kireeva@psuti.ru

Поздняк Ирина Сергеевна, к.т.н., доцент кафедры информационной безопасности ПГУТИ. 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 927 657-24-27. E-mail: i.pozdnyak@psuti.ru

Филиппов Николай Витальевич, студент III курса направления «Информационная безопасность телекоммуникационных систем» факультета телекоммуникаций и радиотехники ПГУТИ. 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 937 984-88-83. E-mail: 170051@edu.psuti.ru

EXPERT SYSTEM APPLICATIONS FOR INDUSTRY-SPECIFIC INFORMATION SECURITY CHALLENGES

Kireeva N.V., Pozdnyak I.S., Filippov N.V.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: kireeva@psuti.ru

The paper addresses the task of studying the parameters of a corporate information security audit. It proposes an expert system database architecture based on the national information security standards and various sectoral requirements. The standards are used to propose ways to populate the expert system's database and the system's modus operandi. It describes the distinctive features of expert system database population in compliance with sectoral requirements, which must provide for some questions and knowledge to be available in the database, which calls for vetting of the system's database content for a specific industry. A user interface algorithm can be used in the context of data security assessment to identify an industry-specific component, which makes it possible to quantify risks and develop recommendations to secure the information system. It also proposes an inference engine design.

Keywords: *database, expert system, industry-specific component, standards, risks, information security*

DOI: 10.18469/ikt.2019.17.4.10

Kireeva Nataliya Valeryevna, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Dean of the Faculty of Telecommunications and Radio Engineering, Associate Professor of Information Security Department. Tel. +7 846 333-13-13. E-mail: kireeva@psuti.ru

Pozdnyak Irina Sergeevna, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Associate Professor of Information Security Department. Tel. +7 927 657-24-27. E-mail: i.pozdnyak@psuti.ru

Filippov Nikolay Vitalievich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; 3rd Year Student of Information Security of Telecommunication Systems Department of Telecommunications and Radio Engineering, Department of Information Security. Tel.: +7 937 984-88-83. E-mail: 170051@edu.psuti.ru

References

1. Sozinova E.N. Primenenie ekspertnyh sistem dlya analiza i ocenki informacionnoj bezopasnosti [The use of expert systems for the analysis and assessment of information security]. *Molodoj uchenyj* [Young Scientist], 2011, no. 10 (33), pp. 61–66. (In Russian).
2. Bubnov D.V. Ekspertnye sistemy kak sredstvo intellektual'noj podderzhki tekhnologicheskih reshenij [Expert systems as a means of intellectual support for technological solutions]. *Vestnik MGTU Stankin* [Bulletin of MSTU Stankin], 2011, no. 4 (16), pp. 83–86. (In Russian).
3. Dzharratano J., Rajli G. *Ekspertnye sistemy: principy razrabotki i programmirovanie / per. s angl.* [Expert systems: principles of development and programming. Trans. from English]. Moscow: Viliams, 2007, 1152 p. (In Russian).
4. Dimov E.M. et al. *Novye informacionnye tekhnologii: podgotovka kadrov i obuchenie personala. Chast' 3. Intellektual'nye infor-macionnye sistemy i upravlenie biznes-processami v infokommunikaciyah* [New Information Technologies: Training and Staff Training. Part 3. Intelligent Information Systems and Business Process Management in Infocommunications]. Samara: Izdatel'stvo SamNC RAN, 2017, 440 p. (In Russian).
5. *GOST R ISO/MEK 27002-2012. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informacionnoj bezopasnosti* [GOST R ISO/MEK 27002-2012. Information technology. Security methods and tools. Code of norms and rules for information security management]. Moscow: Standartinform Publ, 2014, 106 p. (In Russian).
6. *GOST R ISO/MEK 27001-2006. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnosti. Trebovaniya* [GOST R ISO/MEK 27001-2006. Information technology. Security methods and tools. Information security management systems. Requirements]. Moscow: Standartinform Publ, 2008, 31 p. (In Russian).

7. *GOST R ISO/MEK 27005-2010. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informacionnoj bezopasnosti* [GOST R ISO/MEK 27005-2010. Information technology. Security methods and tools. Information Security Risk Management]. Moscow: Standartinform Publ, 2011, 51p. (In Russian).
8. Andrianov V.I., Romanov G.G., Shterenberg S.I. Ekspertnye sistemy v oblasti informacionnoj bezopasnosti [Expert systems in the field of information security]. *IV mezhdunarodnoj nauchno-tekhnicheskoj i nauchno-metodicheskoj konferencii «Aktual'nye problemy info-kommunikacij v nauke i obrazovanii». Sbornik nauchnyh statej* [IV international scientific-technical and scientific-methodical conference «Actual problems of info-communications in science and education». Collection of scientific articles], APINO-2015, Sankt-Peterburg, 2015, vol. 1, pp. 193–197. (In Russian).
9. Korobulina O.Yu. Baza znanij ekspertnoj sistemy audita informacionnoj bezopasnosti [The knowledge base of the expert system for information security audit]. *Programmnye produkty i sistemy* [Software Products and Systems], 2010, no. 4, pp. 89–91. (In Russian).
10. The structure of the expert system. Available at: http://www.aiportal.ru/articles/expert-systems/structure.html (accessed: 23.08.2019). (In Russian).

Received 25.11.2019

ТЕХНОЛОГИИ ЦИФРОВОЙ ЭКОНОМИКИ

УДК 50.03.05

ВЕРОЯТНОСТНОЕ МОДЕЛИРОВАНИЕ УПРАВЛЯЕМОГО ХАОСА

Маслов О.Н.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: maslov@psati.ru

Хаос с позиций теории сложных систем и системного анализа рассматривается как объект, соответствующий области функционирования нерефлекторных сложных систем. Актуальность его изучения объясняется вхождением в триаду «Управляемый хаос – Гибридная война – Цветная революция». Признаком нерефлекторных сложных систем, по определению Н.Н. Моисеева, является наличие «человеческого фактора» в виде лиц, принимающих решения. Для нерефлекторных сложных систем характерны нелинейная динамика и неустойчивое поведение, эффекты самоорганизации в сочетании с хаотическими явлениями и полифуркациями. Неопределенность знаний лиц, принимающих решения о свойствах нерефлекторных сложных систем существенно затрудняет управление ими. Для моделирования хаотических процессов в сложных систем, предлагается использовать достижения теории вероятностей: объективной Лапласа – Колмогорова и субъективной Бернулли – Сэвиджа. Обсуждается соответствие хаотического процесса аксиомам управления, представлена онтологическая модель ситуации, формируемая на базе верифицированных и аксиологических знаний лиц, принимающих решения о параметрах и характеристиках сложных систем. Показана важность структурирования и формализации задач, связанных с исследованием хаотических процессов конкретных сложных систем. Изложены принципы моделирования хаоса с применением аналитических моделей объективной теории вероятностей и эвристических моделей субъективной теории вероятностей. Отмечена перспективность применения новых информационных технологий для анализа и управления хаотическими процессами нерефлекторных сложных систем.

Ключевые слова: *управляемый хаос, анализ и моделирование, теория управления, нерефлекторные системы, человеческий фактор, неопределенность знаний лиц, объективная и субъективная теории вероятностей, фракталы и аттракторы, холоны и акторы, новые информационные технологии*

Введение

Управляемый хаос (Controlled Chaos, от греч. chaos – «беспорядок, неразбериха, путаница») является начальным звеном разрушительной триады, включающей также гибридную войну (Hybrid Warfare) и цветные революции (Coloured Revolution), которая достаточно активно изучается сегодня как в России, так и за рубежом [1]. Противоборство сторон в рамках данной триады соответствует условиям игры с антагонистическими интересами фон Неймана [2] и имеет целью