УДК 004.89
DOI: 10.17586/0021-3454-2020-63-11-1034-1039

АВТОМАТИЗАЦИЯ ЮРИДИЧЕСКОЙ ЭКСПЕРТИЗЫ ТЕКСТОВ ДОГОВОРОВ

К. В. НЕНАУСНИКОВ

Санкт-Петербургский федеральный исследовательский центр Российской академии наук,
199178, Санкт-Петербург, Россия
E-mail: konstantin2113@mail.ru

Выполнено построение модели юридического документа типа „договор“, на основании которого разработана система автоматизации юридической экспертизы. Проанализированы существующие способы автоматической обработки текстов юридических документов, определена их специфика. Для выполнения задачи используется ассоциативно-онтологический подход и применяются методы суммаризации текста. Для упрощения юридической экспертизы текст договора представляется в виде нестрогой последовательности текстовых блоков, каждый из которых отражает независимую от других блоков смысловую нагрузку. Рассматривается задача выделения типовых разделов из текста, описанных посредством набора обязательных и вариативных блоков в порядке их размещения в договоре. Разработана система выделения текстовых блоков, основанная на методах суммаризации и ассоциативно-онтологическом представлении предложений, и предложен алгоритм соотнесения предложений или их частей к одному из типовых блоков. Полученную модель планируется использовать для обработки договоров типа „согласие на обработку персональных данных“.

Ключевые слова: *автоматическая обработка текста, АОТ, legal tech, юридическая экспертиза, соответствие текста, реферирование*

Введение. Работа с договорами — составление, согласование и соблюдение обязательств на протяжении всего срока договора — важный и дорогостоящий процесс, требующий участия одного или нескольких экспертов. Это мониторинг текущего законодательства, вычитка договоров на предмет неправильной структуры и отсутствия неоднозначности, а также отслеживание сроков договоров. Для уменьшения времени выполнения полного цикла обработки договора и снижения сопутствующих затрат могут быть применены методы искусственного интеллекта. Так, применение методов автоматизации возможно на этапах поиска договора, его юридической экспертизы и сопровождения [1].

В настоящей статье рассматриваются вопросы автоматизации юридической экспертизы, целью которой является выявление уязвимых мест и вероятных нарушений. Таковыми могут быть нарушения требований действующего законодательства, например: отсутствие необходимых разделов и формулировок, неправильная структура документа, наличие неоднозначности и др.

В данной области на зарубежном рынке представлены продукты „Thomson Reuters Westlaw“ (https://legal.thomsonreuters.com/en), „Kira Systems“ (https://kirasystems.com/how-it-works/quick-study/), „KM Standards“ (http://knbgmstandards.com/services.html), выполняющие анализ договоров на согласно заданным правилам. Аналогом этих продуктов в России можно считать проект „Система юрист“ компании „Preferentum“ (https://dogovor.1jur.ru/).

В приведенных выше проектах предлагаемые решения направлены на определение типа текста договора, его основных структурных элементов и ключевых для договора объектов (именованных сущностей [2]), также выполняется привязка к близким имеющимся в базе шаблонам. Результат предоставляется пользователю в виде разметки, где определены границы разделов, указаны гиперссылки на связанные разделы и документы, а также предложен список рекомендаций.

Имеющиеся зарубежные проекты ориентированы исключительно на специфику английского текста и неприменимы как к юридическим документам на русском языке, так и, в более широком понимании, к документам, используемым в юридической практике в Российской Федерации.

Существующие решения, созданные для обработки текстов на русском языке, являются проприетарными и в предлагаемых разработчиками демоверсиях не дают возможности загрузки своих документов, что в совокупности не позволяет оценить качество используемых в них моделей и алгоритмов.

Специфика юридических документов. В целом тексты договоров, в отличие от структур общеупотребительной речи, характеризуются меньшим количеством омонимов и замещений терминов местоимениями, что на раннем этапе разработки системы анализа текста снимает необходимость решения задач семантической разметки слов и разрешения местоименной анафоры, а также позволяет использовать терминологические словари.

Другой особенностью юридических документов является сложная синтаксическая структура предложений и практически полное отсутствие размеченных корпусов [3, 4], также, в отличие от других узкоспециализированных областей (медицинской, экономической и т.п.), в области юриспруденции отсутствует общая онтология [5, 6]. Перечисленные свойства не позволяют напрямую применить методы обучения с учителем [7] и классические онтологические подходы [8].

Рассмотрим решение задачи валидации текстового юридического документа, относящегося к договорам.

Определим формально валидацию как процедуру идентификации фрагментов текста, отнесения их к одному из типов, допустимых для данного документа, проверки наличия требуемых фрагментов (текстовых блоков) согласно признакам обязательного наличия, а также порядка следования блоков.

С целью упрощения представим структуру документа типа „договор“ в виде последовательности текстовых блоков. Каждый блок может представлять собой обязательный или вариативный раздел договора, законченное высказывание, несущее независимую от других блоков смысловую нагрузку. Каждый блок может состоять из одного или нескольких предложений, а также быть частью сложного предложения. Разделение естественно-языкового текста на блоки и их дальнейший анализ позволит автоматизировать процесс юридической экспертизы путем выявления обязательных и вариативных разделов документа, их границ и порядка следования, что обусловлено формальными требованиями к структуре документа и в совокупности позволяет упростить для эксперта задачу быстрой проверки документа на корректность.

Часть блоков имеет однозначное расположение в тексте, например, наименование договора (блок *1*), как правило, стоит в начале текста, а дата и подпись (блок *n*) в конце. Другие блоки в разных вариантах договора могут в пределах определенного отрывка располагаться в случайном порядке, так, на рис. 1 отрывок 2 содержит блоки *2*, *3* и *4*, а отрывок 3 — блоки *5* и *6*. Порядок блоков внутри отрывка может быть произвольным, что не влияет на корректность текста договора.

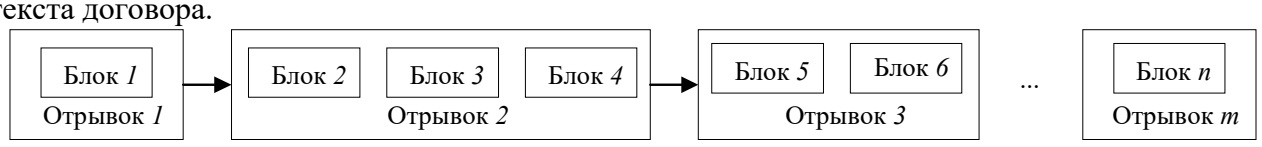

Рис. 1

Для учета требований к последовательности блоков вводится проверка на последовательность условных номеров блоков *N*, заданных в общем шаблоне документа. Шаблон договора включает в себя список разделов, где каждый раздел содержит свой номер, имя, тип (обязательный или вариативный) и примеры использования, заданные в виде графа связности (рис. 2).

Корректным считается текст, в котором для каждого блока с номером N_B выполняется условие $N_A < N_B$, где N_A — номер любого блока, находящегося перед блока с номером N_B. Если положение блока в тексте неважно, то такой блок не имеет собственного значения N и в проверке не участвует.

Рис. 2

Зависимость блоков определяется их положением в тексте. Блок, который зависит от впередистоящего, в тексте может располагаться только после него. Для примера, на рис. 2 корректный порядок блоков в тексте может быть представлен тремя комбинациями: (*A*, *B*, *C*, *D*), (*C*, *A*, *B*, *D*) и (*A*, *C*, *B*, *D*).

Система поддержки юридической экспертизы. Юридическая экспертиза выполняется с учетом существующего законодательства, „полезных юридических практик“ и коллекции верно построенных документов — на основании этого набора составляются формальные требования к документу. Также на этом основании выполняются разделение текста договора на блоки и анализ их принадлежности к обязательному списку разделов. В дальнейшем согласно найденным несоответствиям генерируются рекомендации к исправлению. Функциональная модель системы поддержки юридической экспертизы представлена на рис. 3.

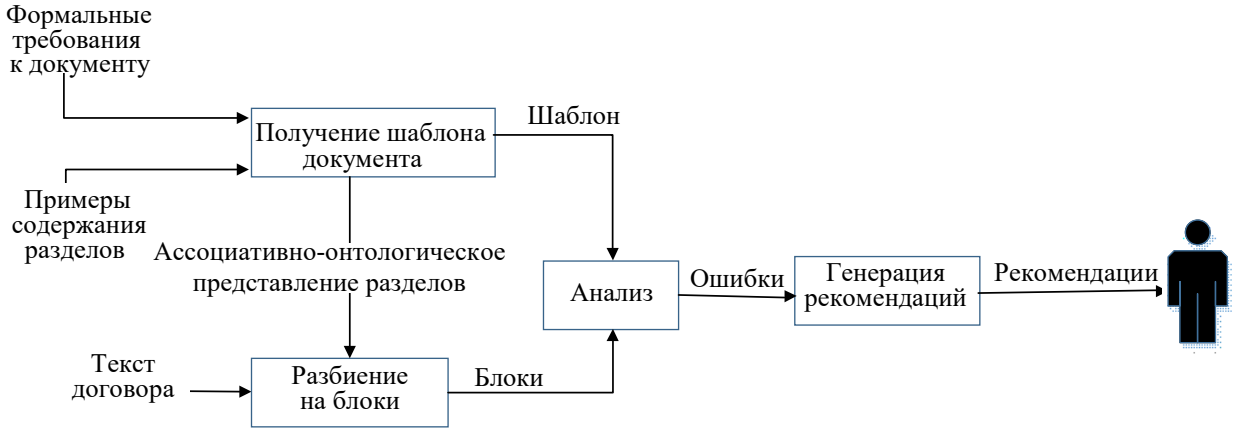

Рис. 3

В случае отсутствия разметки и онтологии для формирования шаблона можно использовать методы на основе ассоциативно-онтологического подхода [9].

Для определения границ блоков может быть использован метод реферирования. Основным структурным элементом при выполнении реферирования считаются предложения [10]. Положение блока определяется в два этапа. На первом этапе оценивается близость каждого предложения к каждому из блоков шаблона, затем предложения с наиболее высокой оценкой близости вычеркиваются. Процесс повторяется для оставшегося текста. Таким образом, несколько предложений могут содержать элементы одного блока, но несколько блоков не могут относится к одному предложению.

На втором этапе, если остались незадействованные блоки, начинается проверка возможности того, что предложение содержит два блока. Для этого предложение разбивается на две равные части, при этом середина предложения определяется по количеству содержащихся в нем слов без учета знаков препинания. Затем определяется максимум суммы двух вероятностей принадлежности частей предложения к блокам путем последовательных сдвигов границы раздела предложения на одно слово. В случае если максимум суммы двух вероятностей пре-

вышает вероятность принадлежности исходного предложения к первоначальному блоку, то предложение представляется в виде двух определенных фрагментов (рис. 4).

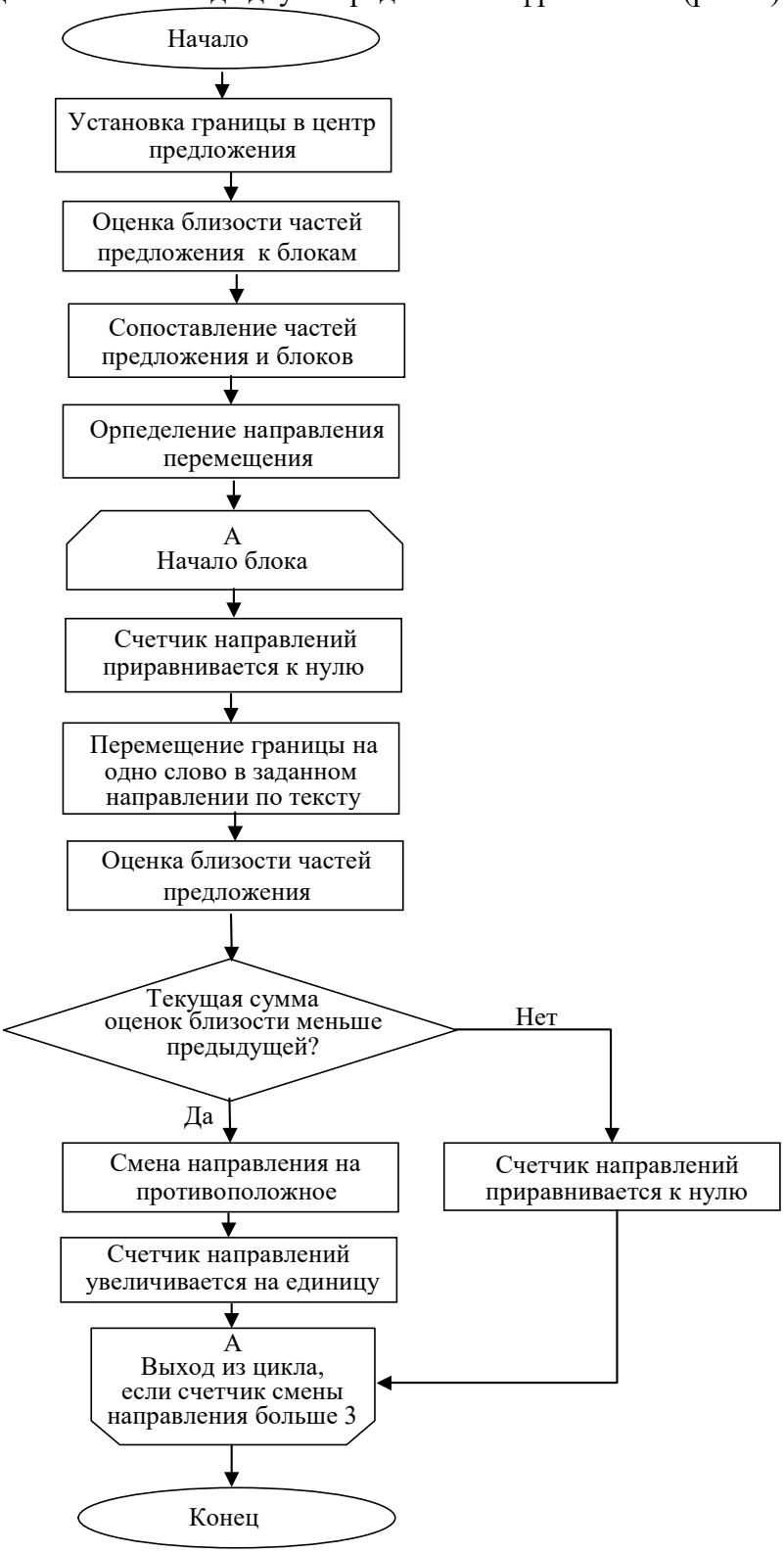

Рис. 4

На основании выделенных из текста рассматриваемого документа и имеющегося шаблона блоков выполняется анализ. Определяется список ошибок, содержащихся в тексте.

Заключение. Представлен обзор существующих решений для анализа юридических документов и выполнено построение модели текста типа „договор“ с целью автоматизации процесса юридической экспертизы.

На основе разработанной модели построена система поддержки юридической экспертизы, позволяющая выполнить разделение текста на блоки, соответствующие пунктам экспертного шаблона. Рассмотрены отдельные части общей задачи валидации юридического документа, включая задачу определения границ блоков текста и проверки их последовательности

Построенную модель договора и систему поддержки юридической экспертизы в дальнейшем планируется применить для анализа качества договоров типа „Согласие на обработку персональных данных“.

Работа выполнена в рамках реализации Государственного задания на 2020 г., № 0073-2019-0005.

СПИСОК ЛИТЕРАТУРЫ

1. *Grossman M., Cormack G.* Technology-assisted review in E-discovery can be more effective and more efficient than exhaustive manual review // Richmond Journal of Law and Technology. 2011. Vol. 17, N 3.
2. *Lample G., Ballesteros M., Subramanian S., Kawakami K., Dyer C.* Neural architectures for named entity recognition // Proc. of the Conf. of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL HLT 2016). 2016. P. 260—270. DOI: 10.18653/v1/N16-1030.
3. *Cardellino C., Alemany L. A., Teruel M., Villata S., Marro S.* Convolutional ladder networks for legal NERC and the impact of unsupervised data in better generalizations // Proc. of the 32nd Intern. Florida Artificial Intelligence Research Society Conf. (FLAIRS-32). 2016. P. 155—160.
4. *Zhang J., El-Gohary N. M.* Semantic NLP-based information extraction from construction regulatory documents for automated compliance checking // J. of Computing in Civil Engineering. 2013. Vol. 30, N 2. DOI: 10.1061/(ASCE)CP.1943-5487.0000346.
5. *Ajani G., Boella G., Caro D. L., Robaldo L., Humphreys L., Praduroux S., Rossi P., Violato A.* The european legal taxonomy syllabus: a multi-lingual, multi-level ontology framework to untangle the web of european legal terminology // App. Ontology. 2016. Vol. 11. P. 325—375. DOI: 10.3233/AO-170174.
6. *Soysal E., Cicekli I., Baykal N.* Design and evaluation of an ontology based information extraction system for radiological reports // Computers in Biology and Medicine. 2010. Vol. 40, N 11. P. 900—911. DOI: 10.1016/j.compbiomed.2010.10.002.
7. *Blums I., Weigand H.* Towards a reference ontology of complex economic exchanges for accounting information systems // IEEE 20th Intern. Enterprise Distributed Object Computing Conf. (EDOC) 2016. P. 1—10. DOI: 10.1109/EDOC.2016.7579388.
8. *Devlin J., Chang M.W., Lee K., Toutanova K.* BERT: Pre-training of deep bidirectional transformers for language understanding // Proc. of the Conf. of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL HLT 2019). 2019. Vol. 1. P. 4171—4186.
9. *Kuleshov S., Zaytseva A., Aksenov A.* Natural language search and associative-ontology matching algorithms based on graph representation of texts // Advances in Intelligent Systems and Computing. 2019. Vol. 1046. DOI: 10.1007/978-3-030-30329-7_26.
10. *Allahyari M., Pouriyeh S., Assefi M.* et al. Text summarization techniques: a brief survey // Intern. Journal of Advanced Computer Science and Applications. 2017. Vol. 8, N 10. DOI: 10.14569/ijacsa.2017.081052.

Сведения об авторе

Константин Вячеславович Ненаусников — СПбФИЦ РАН, СПИИРАН, лаборатория автоматизации научных исследований; мл. научный сотрудник;
E-mail: konstantin2113@mail.ru

Поступила в редакцию
02.10.2020 г.

Ссылка для цитирования: *Ненаусников К. В.* Автоматизация юридической экспертизы текстов договоров // Изв. вузов. Приборостроение. 2020. Т. 63, № 11. С. 1034—1039.

AUTOMATION OF LEGAL EXPERTISE OF AGREEMENT TEXTS

K. V. Nenausnikov

St. Petersburg Federal Research Center of the RAS,
199178, St. Petersburg, Russia
E-mail: konstantin2113@mail.ru

A model of a legal document of the “contract” type is built and used as the basis of a system developed for legal expertise automation. The existing methods of automatic processing of texts of legal documents are analyzed, their specificity is determined. To accomplish the task, an associative-ontological approach is used, and methods of text summarization are applied. To simplify the legal examination, the text of the agreement is presented in the form of a non-strict sequence of text blocks, each of which reflects a semantic load independent of other blocks. The problem of highlighting typical sections from the text, described by means of a set of mandatory and variable blocks in the order of their placement in the contract, is considered. A system for the text blocks selection is been developed based on the methods of summarization and associative-ontological representation of sentences. An algorithm for correlating sentences or their parts to one of standard blocks is proposed. The resulting model is planned to be used for processing agreements of the "consent to the processing of personal data" type.

Keywords: automated text processing, legal tech, legal expertise, text compliance, text summarization

REFERENCES

1. Grossman M., Cormack G. *Richmond Journal of Law and Technology,* 2011, no. 3(17).
2. Lample G., Ballesteros M., Subramanian S., Kawakami K., Dyer C. *Proceedings of the Conference of the North American Chapter of the Association for Computational Linguistics*, Human Language Technologies (NAACL HLT-2016), 2016, pp. 260–270, DOI: 10.18653/v1/N16-1030.
3. Cardellino C., Alemany L.A., Teruel M., Villata S., Marro S. *Proceedings of the 32nd International Florida Artificial Intelligence Research Society Conference (FLAIRS-32)*, 2016, pp. 155–160.
4. Zhang J., El-Gohary N.M. *Journal of Computing in Civil Engineering*, 2013, no. 2(30), DOI: 10.1061/(ASCE)CP.1943-5487.0000346.
5. Ajani G., Boella G., Caro D.L., Robaldo L., Humphreys L., Praduroux S., Rossi P., Violato A. *Applied ontology*, 2016, vol. 11, pp. 325–375, DOI: 10.3233/AO-170174.
6. Soysal E., Cicekli I., Baykal N. *Computers in Biology and Medicine,* 2010, no. 11(40), pp. 900–911, DOI: 10.1016/j.compbiomed.2010.10.002.
7. Blums I., Weigand H. *IEEE 20th International Enterprise Distributed Object Computing Conference (EDOC),* 2016, pp. 1–10, DOI: 10.1109/EDOC.2016.7579388.
8. Devlin J. Chang M.W., Lee K., Toutanova K. *Proceedings of the Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL HLT 2019),* 2019, vol. 1, pp. 4171–4186.
9. Kuleshov S., Zaytseva A., Aksenov A. *Intelligent Systems Applications in Software Engineering. CoMeSySo 2019,* Advances in Intelligent Systems and Computing, Springer, Cham, 2019, vol. 1046, DOI 10.1007/978-3-030-30329-7_26.
10. Allahyari M., Pouriyeh S., Assefi M., Safaei S., Trippe E. D., Gutierrez J. B., Kochut K. *International Journal of Advanced Computer Science and Applications,* 2017, no. 10(8), DOI: 10.14569/ijacsa.2017.081052.

Data on author

Konstantin V. Nenausnikov — St. Petersburg Federal Research Center of the RAS, St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Research Automation; Junior Researcher; E-mail: konstantin2113@mail.ru

For citation: Nenausnikov K. V. Automation of legal expertise of agreement texts. *Journal of Instrument Engineering*. 2020. Vol. 63, N 11. P. 1034—1039 (in Russian).

DOI: 10.17586/0021-3454-2020-63-11-1034-1039

УДК 004.056.53
DOI: 10.17586/0021-3454-2020-63-11-1040-1045

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ПРОЦЕССУ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Д. С. Левшун

Санкт-Петербургский федеральный исследовательский центр Российской академии наук, 199178, Санкт-Петербург, Россия
E-mail: levshun@comsec.spb.ru
Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: levshun@itmo.ru

Представлен подход к формированию требований при проектировании защищенных киберфизических систем. Данный подход является одним из этапов разрабатываемой автором методики проектирования и верификации подобных систем. В ходе этого этапа пожелания заказчика преобразуются в конкретные требования и ограничения, на основе которых строится процесс проектирования. Преобразование происходит на основе сформированной базы знаний. В качестве примера представлен процесс формирования требований к проектированию мобильного робота для охраны периметра объекта.

Ключевые слова: *безопасность в соответствии с проектом, киберфизическая система, пожелания заказчика, формирование требований*

Введение. В настоящее время киберфизические системы — это неотъемлемая часть любой сферы жизнедеятельности человека, что обусловливает критическую важность обеспечения их защищенности. Последствия отказа подобных систем, в том числе связанные с деятельностью злоумышленников, включают в себя как финансовый и репутационный ущерб, так и угрозу жизни и здоровью человека. Одним из возможных направлений атаки является использование уязвимостей, наличие которых в киберфизических системах обусловлено различными факторами. Наиболее опасные из них — внесенные из-за ошибок на этапе проектирования.

Для решения данной проблемы разработаны и применяются на практике различные методики [1], описывающие подходы к проектированию аппаратных и программных элементов [2—5], протоколов и интерфейсов [6—8], программно-аппаратных элементов [9—11], среды передачи данных [12, 13] или системы в целом [14, 15].

Основной недостаток подобных решений заключается в рассмотрении только отдельных аспектов обеспечения безопасности, что не позволяет применить их для киберфизических систем в целом. К примеру, в подходах к проектированию программных элементов не учитывается, что отдельные компоненты киберфизических систем имеют сильную связь между аппаратной и программной составляющими. Это особенно характерно для устройств на основе микроконтроллеров, проектирование которых связано с рядом ограничений. Недостатком подходов к проектированию отдельных устройств (программно-аппаратных элементов) является анализ защищенности без учета особенностей системы в целом, что может привести к небезопасной среде передачи данных. При этом совместное применение отдельных подходов представляется сложной задачей [16, 17].

Один из ключевых этапов методик проектирования — формирование требований. В ходе этого этапа пожелания заказчика преобразуются в функциональные требования и ограничения, на основе которых строится процесс проектирования. Как правило, данное преобразование происходит на основе сформированной базы знаний.

Подход к формированию требований. Процесс формирования требований к проектированию защищенных киберфизических систем состоит из следующих шагов:

— устанавливается взаимосвязь между *пожеланиями* заказчика и общими *задачами*, решение которых должна обеспечивать проектируемая система;

— сформированный на предыдущем шаге список общих *задач* преобразуется в *возможности*, которыми должна обладать проектируемая система;

— сформированный на предыдущем шаге список *возможностей* преобразуется в конкретные *требования* к проектируемой системе.

В свою очередь, каждое из сформированных *требований* связано с наличием различных *компонентов* системы, используемых при проектировании. Обобщенная схема предлагаемого подхода представлена на рис. 1.

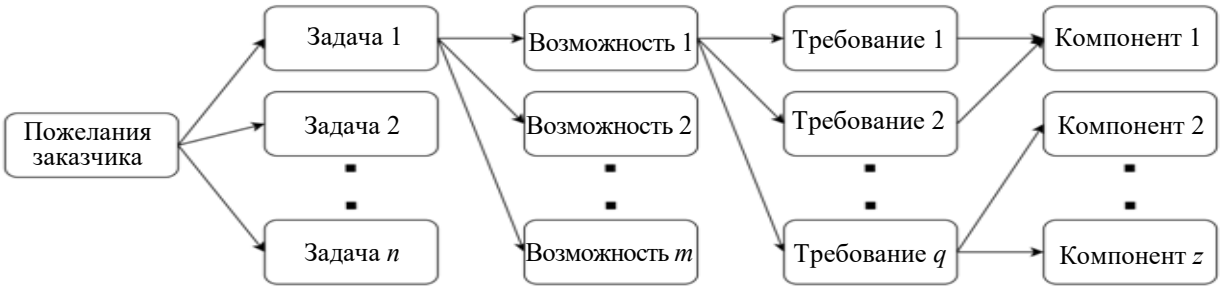

Рис. 1

Отметим, что в данной схеме не учитывается взаимосвязь между отдельными задачами и возможностями — вполне реальна ситуация, когда решение одной задачи зависит от другой, что в итоге формирует иерархическую структуру требований. При этом каждый из указанных процессов основан на работе с базой знаний, поэтому качество получаемых результатов напрямую зависит от ее полноты.

Формирование требований к мобильному роботу. Рассмотрим процесс формирования требований к такой киберфизической системе, как мобильный робот для мониторинга периметра объекта. Отметим, что элементы корпуса робота были известны заранее, поэтому их параметры были использованы для формирования ограничений по размеру используемых сенсоров, а также для вычисления минимальной достаточной мощности используемых моторов. Более того, такие требования, как наличие аккумулятора, интерфейса для подзарядки, системы управления и хранения данных, рассматривались по умолчанию и соответственно не анализировались более детально.

Пожелания заказчика о проектировании мобильного робота для мониторинга периметра объекта в соответствии с предлагаемым подходом были интерпретированы как следующие общие задачи: мобильный робот должен иметь возможность поддерживать собственный рабочий цикл, осуществлять мониторинг периметра, а также взаимодействовать с нарушителем периметра и оператором системы. Взаимосвязь общих задач с возможностями киберфизической системы и конкретными требованиями к ней представлена в таблице (в графе „Требования“ — наличие элементов и алгоритмов).

Основная идея процесса проектирования — поиск всех альтернатив компонентного состава системы, удовлетворяющих сформированным *требованиям*. В свою очередь, соответствие всем *требованиям* означает, что спроектированная система обладает необходимыми *возможностями* для решения поставленных *задач*. А если система способна решить все поставленные *задачи*, то это именно та система, которая нужна заказчику, при условии, что база знаний заполнена корректно. Так, для приведенного выше примера, каждое сформированное *требование* может быть удовлетворено с помощью различных аппаратных и программных элементов. Например, шасси может иметь одно или несколько колес или гусениц, а от выбранного решения будет зависеть количество необходимых моторов.

Общие задачи	Возможности	Требования	Зависимости
Поддержка рабочего цикла	Движение	Шасси	—
		Моторы для перемещения шасси	
		Алгоритм движения	
		Алгоритм построения оптимального пути	
	Обход препятствий	Сенсоры обнаружения препятствий	Для возможности **обхода препятствия** робот должен иметь возможность **двигаться**
		Моторы для перемещения сенсоров	
		Алгоритм обнаружения препятствий	
		Алгоритм обхода препятствий	
	Подзарядка	Мониторинг заряда батареи	Для возможности **подзарядки** робот должен иметь возможность **двигаться** и **обходить препятствия**
		Наличие станций подзарядки	
		Алгоритм подзарядки	
Мониторинг периметра объекта	Формирование представления об окружающей среде	Сенсоры для сканирования окружающей среды	Для возможности **формирования представления об окружающей среде** задача **поддержки рабочего цикла** должна быть решена
		Моторы для перемещения сенсоров	
		Алгоритм обработки данных об окружающей среде	
		Алгоритм построения карты окружающей среды	
Взаимодействие с нарушителем	Обнаружение нарушителя	Сенсоры для обнаружения нарушителя	Для возможности **обнаружения нарушителя** задача **мониторинга периметра** должна быть решена
		Моторы для перемещения сенсоров	
		Алгоритм обнаружения нарушителя	
		Алгоритм распознавания нарушителя	
	Преследование нарушителя	Алгоритм определения направления движения нарушителя	Для возможности **преследования нарушителя** робот должен иметь возможность **обнаруживать нарушителя,** а задача **мониторинга периметра** должна быть решена
		Алгоритм преследования	
Взаимодействие с оператором	Взаимодействие с оператором	Интерфейс взаимодействия	Для возможности **взаимодействия с оператором** задача **поддержки рабочего цикла** должна быть решена
		Алгоритм взаимодействия	

В то же время некоторые аппаратные элементы могут быть использованы для удовлетворения сразу нескольких *требований*: сенсоры для сканирования окружающей среды могут быть также задействованы для обнаружения препятствий и нарушителей. Более того, применение определенных алгоритмов может повлечь за собой новые требования: например, при формировании представления об окружающей среде могут быть использованы данные, полученные от определенных сенсоров. При этом существуют иерархические зависимости между *общими задачами* и *возможностями*, которые отражены на рис. 2.

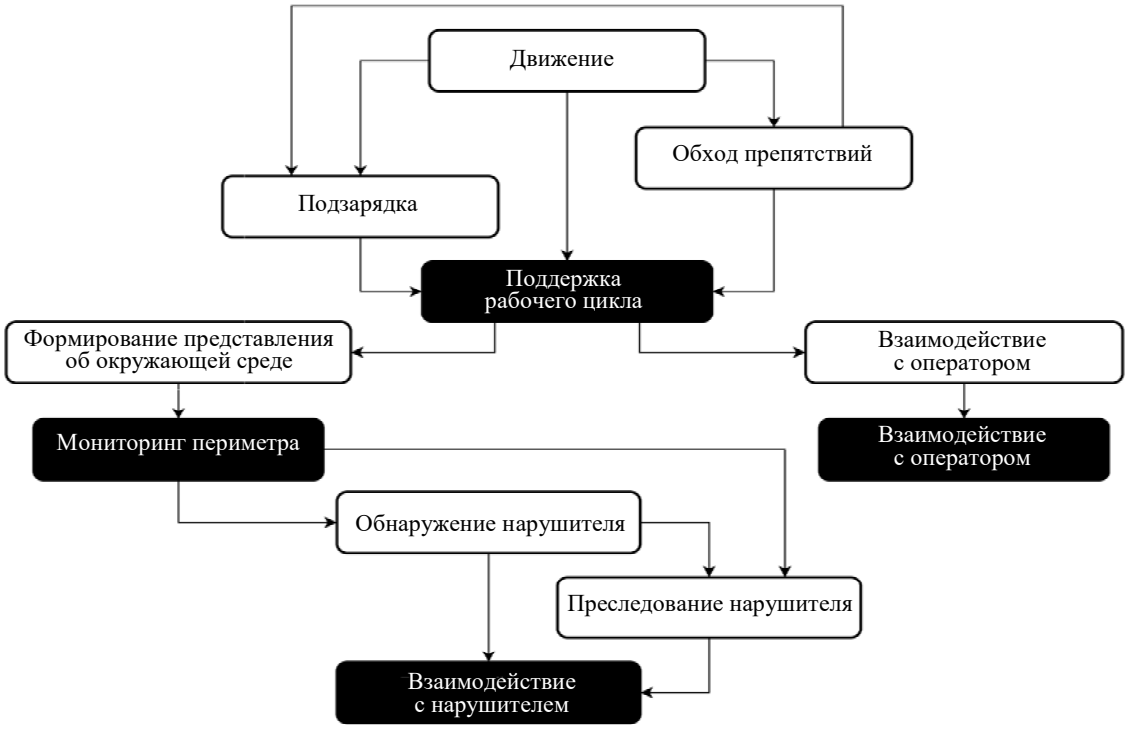

Рис. 2

Это означает, что при проектировании киберфизических систем важно учитывать различные зависимости между их элементами, точно так же как возможные конфликты и несовместимости.

Заключение. Понимание зависимостей между сформированными общими задачами, возможностями и требованиями, а также различными компонентами киберфизических системы, которые необходимы для их реализации, позволяет сформировать процесс построения защищенной системы шаг за шагом и сократить количество ситуаций, связанных с пересмотром принятых решений, что значительно ускоряет процесс проектирования.

Представленный подход является частью методики проектирования и верификации киберфизических систем, исследование и разработка которой ведется автором в настоящее время. Ключевая идея данной методики заключается в предоставлении автоматизированного инструмента для проектирования защищенных киберфизических систем. Предполагается, что использование подобного инструмента позволит уменьшить количество ошибок, возникающих при проектировании, что, в свою очередь, позволит снизить количество уязвимостей в киберфизических системах. Снижение количества уязвимостей позволит уменьшить риски, связанные с финансовыми и временными затратами, а также риски, связанные с безопасностью людей.

Одной из особенностей разрабатываемой методики является интеграция процесса верификации киберфизических систем в качестве неотъемлемой ее части. Верификация позволяет осуществить формальную проверку возможности проектирования системы в соответствии со сформированными требованиями, а также обеспечить защищенность системы от злоумышленника, обладающего определенным набором знаний и ресурсов. При этом важно отметить, что методика не ставит своей целью замену эксперта по безопасности, однако позволит избавить его от части рутинных задач, связанных с формированием альтернатив компонентному составу системы с учетом возможных конфликтов и несовместимостей.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90082 и бюджетной темы 0073-2019-0002.

СПИСОК ЛИТЕРАТУРЫ

1. *Левшун Д. С., Котенко И. В., Чечулин А. А.* Методика проектирования и верификации защищенных киберфизических систем // Вестн. Санкт-Петербургского гос. ун-та технологии и дизайна. Сер. 1. Естественные и технические науки. 2019. № 4. С. 19—22.

2. *Shamal F.* Further applications of CAIRIS for usable and secure software design // Designing Usable and Secure Software with IRIS and CAIRIS / Ed. *F. Shamal.* Springer, Cham, 2018. P. 239—254.

3. *Kobashi T., Washizaki H., Yoshioka N., Kaiya H., Okubo T., Fukazawa Y.* Designing secure software by testing application of security patterns // Exploring Security in Software Architecture and Design. IGI Global, 2019. P. 136—169.

4. *Ardeshiricham A., Hu W., Marxen J., Kastner R.* Register transfer level information flow tracking for provably secure hardware design // Design, Automation & Test in Europe, DATE 2017. Conference & Exhibition IEEE, Lauzanne, Switzerlang, 23—31 March. 2017. P. 1691—1696.

5. *Zhang D., Wang Y., Suh G. E., Myers A. C.* A hardware design language for timing-sensitive information-flow security // ACM Sigplan Notices. 2015. Vol. 50, N 4. P. 503—516.

6. *Xu X., He B., Yang W., Zhou X., Cai Y.* Secure transmission design for cognitive radio networks with Poisson distributed eavesdroppers // IEEE Trans. on Information Forensics and Security. 2015. Vol. 11, N 2. P. 373—387.

7. *Wang B., Zhong S. M., Dong X. C.* On the novel chaotic secure communication scheme design // Communications in Nonlinear Science and Numerical Simulation. 2016. Vol. 39. P. 108—117.

8. *Takahashi S., Ikeda T., Shinagawa Y., Kunii T. L., Ueda M.* Algorithms for extracting correct critical points and constructing topological graphs from discrete geographical elevation data // Computer Graphics Forum. Edinburgh, UK: Blackwell Science Ltd, 1995. Vol. 14, N 3. P. 181—192.

9. *Wang Z., Karpovsky M., Bu L.* Design of reliable and secure devices realizing Shamir's secret sharing // IEEE Trans. on Computers. 2015. Vol. 65, N 8. P. 2443—2455.

10. *Scott-Hayward S.* Design and deployment of secure, robust, and resilient SDN Controllers // Proc. of the 1st IEEE Conf. on Network Softwarization (NetSoft). 2015. P. 1—5.

11. *Desnitsky V., Levshun D., Chechulin A., Kotenko I.* Design technique for secure embedded devices: application for creation of integrated cyber-physical security system // JoWUA. 2016. Vol. 7, N 2. P. 60—80.

12. *Saleem K., Derhab A., Al-Muhtadi J., Shahzad B.* Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society // Computers in Human Behavior. 2015. Vol. 51. P. 977—985.

13. *Huang J., Huang C. T.* Secure mutual authentication protocols for mobile multi-hop relay WiMAX networks against rogue base/relay stations // IEEE Intern. Conf. on Communications (ICC). 2011. P. 1—5.

14. *Penas O., Plateaux R., Patalano S., Hammadi M.* Multi-scale approach from mechatronic to Cyber-Physical Systems for the design of manufacturing systems // Computers in Industry. 2017. Vol. 86. P. 52—69.

15. *Lin Z., Yu S., Lü J., Cai S., Chen G.* Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system // IEEE Trans. on Circuits and Systems for Video Technology. 2014. Vol. 25, N 7. P. 1203—1216.

16. *Левшун Д. С., Чечулин А. А., Котенко И. В.* Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Тр. учебных заведений связи. 2019. Т. 5, № 4. С. 114—123. DOI:10.31854/1813-324X-2019-5-4-113-122.

17. *Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В.* Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Тр. СПИИРАН. 2016. Т. 48, № 5. С. 5—31. DOI: 10.15622/sp.48.1.

Сведения об авторе

Дмитрий Сергеевич Левшун — СПбФИЦ РАН, СПИИРАН, лаборатория проблем компьютерной безопасности; мл. научный сотрудник; Университет ИТМО, факультет безопасности информационных технологий; аспирант;
E-mail: levshun@comsec.spb.ru, levshun@itmo.ru

Поступила в редакцию
02.10.2020 г.

Ссылка для цитирования: *Левшун Д. С.* Формирование требований к процессу проектирования защищенных киберфизических систем // Изв. вузов. Приборостроение. 2020. Т. 63, № 11. С. 1040—1045.

FORMATION OF REQUIREMENTS FOR THE DESIGN PROCESS OF SECURE CYBER-PHYSICAL SYSTEMS

D. S. Levshun

St. Petersburg Federal Research Center of the RAS,
199178, St. Petersburg, Russia
E-mail: levshun@comsec.spb.ru
ITMO University, 197101, Saint Petersburg, Russia
E-mail: levshun@itmo.ru

An approach to formation of requirements for the design process of secure cyber-physical systems is described. This approach covers one of the stages of the design and verification methodology for such systems. During this stage, the customer's wishes are transformed into specific requirements and constraints, which determines the design process. The transformation is performed based on the formed knowledge base. As an example of the approach application, the process of forming requirements for the design of a mobile robot for an object perimeter monitoring is presented.

Keywords: security by design, cyber-physical system, customer's wishes, requirements formation

REFERENCES

1. Levshun D.S., Kotenko I.V., Chechulin A.A. *Vestnik of St. Petersburg State University of Technology and Design Series 1. Natural and technical science*, 2019, no. 4, pp. 19–22. (in Russ.)
2. Shamal Faily. *Further Applications of CAIRIS for Usable and Secure Software Design. Designing Usable and Secure Software with IRIS and CAIRIS*, Springer, Cham, 2018, pp. 239–254.
3. Kobashi T., Washizaki H., Yoshioka N., Kaiya H., Okubo T., Fukazawa Y. *Exploring Security in Software Architecture and Design*, IGI Global, 2019, pp. 136–169.
4. Ardeshiricham A., Hu W., Marxen J., Kastner R. *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2017, IEEE, 2017, pp. 1691–1696.
5. Zhang D., Wang Y., Suh G.E., Myers A.C. *ACM Sigplan Notices*, 2015, no. 4(50), pp. 503–516.
6. Xu X., He B., Yang W., Zhou X., Cai Y. *IEEE Transactions on Information Forensics and Security*, 2015, no. 2(11), pp. 373–387.
7. Wang B., Zhong S.M., Dong X.C. *Communications in Nonlinear Science and Numerical Simulation*, 2016, vol. 39, pp. 108–117.
8. Takahashi S., Ikeda T., Shinagawa Y., Kunii T.L., Ueda M. *Computer Graphics Forum*, Edinburgh, UK: Blackwell Science Ltd, 1995, no. 3(14), pp. 181–192.
9. Wang Z., Karpovsky M., Bu L. *IEEE Transactions on Computers*, 2015, no. 8(65), pp. 2443–2455.
10. Scott-Hayward S. *Proceedings of the 1st Conference on Network Softwarization (NetSoft)*, IEEE, 2015, pp. 1–5.
11. Desnitsky V., Levshun D., Chechulin A., Kotenko I. *Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System. JoWUA*, 2016, no. 2(7), pp. 60–80.
12. Saleem K., Derhab A., Al-Muhtadi J., Shahzad B. *Computers in Human Behavior*, 2015, vol. 51, pp. 977–985.
13. Huang J., Huang C.T. *International Conference on Communications (ICC)*, IEEE, 2011, pp. 1–5.
14. Penas O., Plateaux R., Patalano S., Hammadi M. *Computers in Industry*, 2017, vol. 86, pp. 52–69.
15. Lin Z., Yu S., Lü J., Cai S., Chen G. *IEEE Transactions on Circuits and Systems for Video Technology*, 2014, no. 7(25), pp. 1203–1216.
16. Levshun D.S Chechulin A.A., Kotenko I.V. *Proceedings of Telecommunication Universities*, 2019, no. 4(5), pp. 114–123, DOI:10.31854/1813-324X-2019-5-4-113-122. (in Russ.)
17. Desnitsky V., Chechulin A., Kotenko I., Levshun D., Kolomeec M. *Informatics and Automation (SPIIRAS Proceedings)*, 2016, no. 5(48), pp. 5–31, DOI: 10.15622/sp.48.1.

Data on author

Dmitry S. Levshun — St. Petersburg Federal Research Center of the RAS, St. Petersburg Institute for Informatics and Automation of the RAS, Laboratory of Computer Security Problems; Junior Researcher; ITMO University, Faculty of Secure Information Technologies; Post-Graduate Student; E-mail: levshun@comsec.spb.ru, levshun@itmo.ru

For citation: Levshun D. S. Formation of requirements for the design process of secure cyber-physical systems. *Journal of Instrument Engineering*. 2020. Vol. 63, N 11. P. 1040—1045 (in Russian).

DOI: 10.17586/0021-3454-2020-63-11-1040-1045