

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 обуславливает 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.

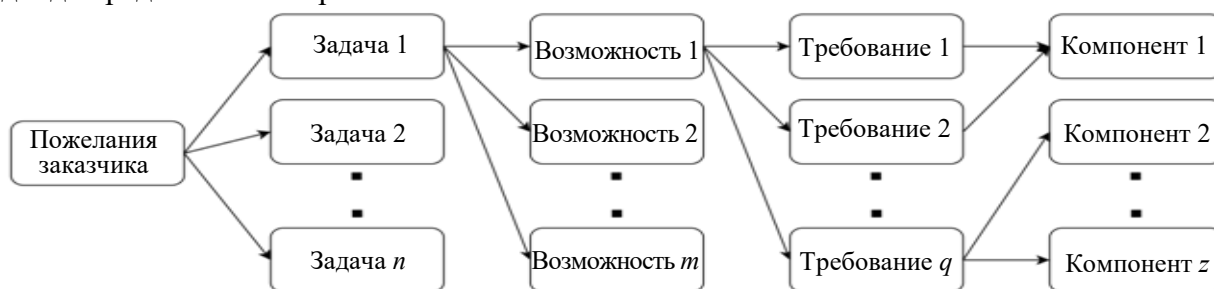


Рис. 1

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.

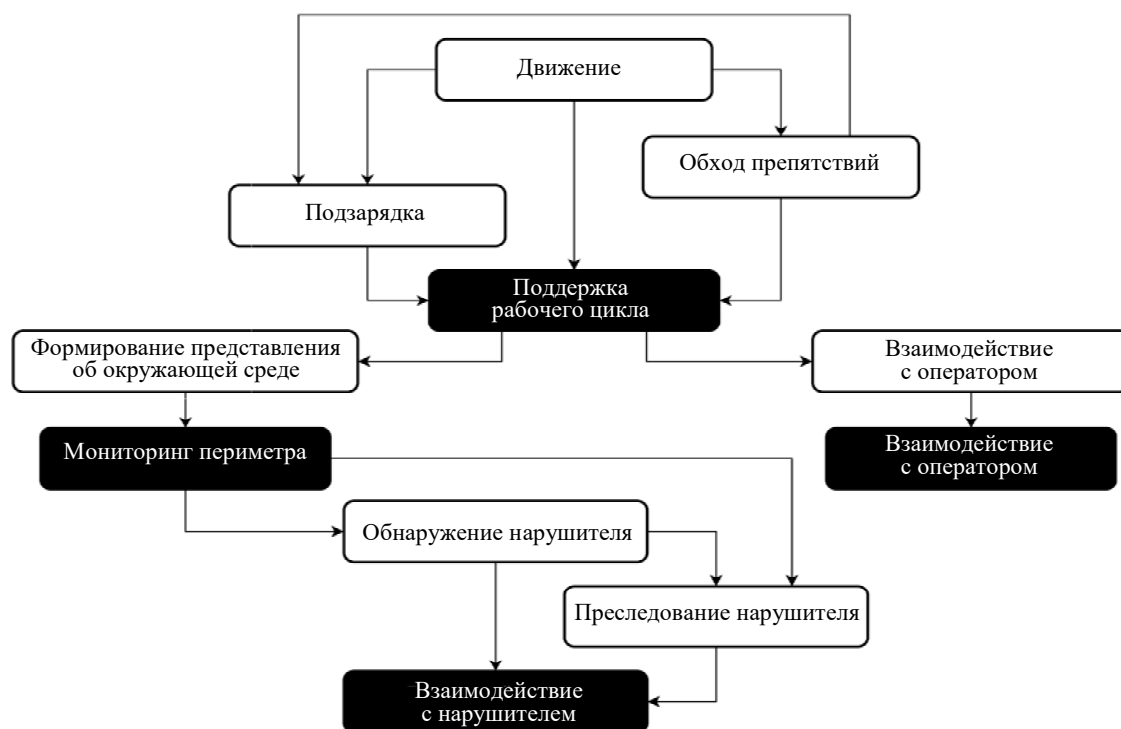


Рис. 2

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, Lausanne, Switzerland, 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

ЭФФЕКТИВНОСТЬ ВИЗУАЛИЗАЦИИ ДАННЫХ В ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

М. В. КОЛОМЕЕЦ

*Санкт-Петербургский федеральный исследовательский центр Российской академии наук,
199178, Санкт-Петербург, Россия
E-mail: kolomeec@comsec.spb.ru*

Представлены результаты экспериментов по тестированию восприятия 12 компонентов визуализации в виртуальной реальности на основе слепого тестирования 20 пользователей. Тестирование производилось с использованием очков и контроллеров виртуальной реальности HTC Vive. Проведена оценка скорости и точности восприятия визуализации 9 численных и 3 категориальных компонентов. На основе верхнего квантиля распределения оценок определены компоненты, рекомендуемые к использованию в системах визуальной аналитики. Полученные оценки скорости и точности интерпретации информации позволяют учитывать особенности восприятия при проектировании систем анализа, использующих виртуальную реальность.

Ключевые слова: *визуальная аналитика, виртуальная реальность, анализ данных, оценка эффективности восприятия, слепое тестирование*

По аналогии с визуальной аналитикой в пространстве 2D процесс визуализации данных в виртуальной реальности включает множество компонентов, из которых складывается изображение, — графических примитивов, таких как точки, фигуры, цвета и т.д. При этом восприятие пользователем изображения в 2D и в 3D значительно различается. Для того чтобы иметь возможность разрабатывать эффективные системы анализа с поддержкой виртуальной реальности необходимо иметь представление об эффективности компонентов изображения. Таким образом, возникает необходимость изучить эффективность восприятия базовых компонентов визуализации.

Эффективность визуализации сложно оценить [1] и формализовать, так как зачастую такая оценка носит субъективный характер. Тем не менее можно выделить два объективных измеряемых показателя: точность интерпретации информации и скорость принятия решения.

В общих чертах процесс визуализации и принятия решений представлен на рис. 1. Метрика (например, число 15) преобразуется в графический компонент (например, куб объемом, равным 15). Пользователь изучает куб и пытается интерпретировать его размер; он дает ответ (например, 14) и тратит какое-то время на принятие решения (например, 10 с). Таким образом, эффективность выражается в точности и скорости интерпретации метрики — разнице между фактическим значением и ответом пользователя.

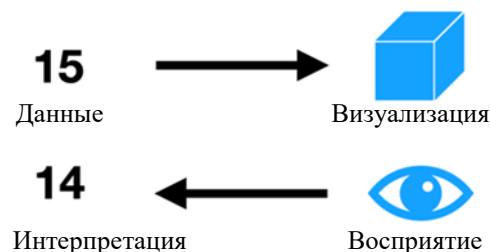


Рис. 1

По точности интерпретации [2] компонентов их можно разделить на 1) точные — рекомендуемые к использованию для визуализации точных метрик; 2) с погрешностями — реко-

мендуемые к использованию для визуализации неточных метрик; 3) неточные — не рекомендуемые к использованию.

По скорости восприятия компонентов их можно разделить на 1) быстрые — рекомендуемые к использованию для привлечения внимания; 2) приемлемые — рекомендуемые к использованию для быстрого принятия решений; 3) медленные — не рекомендуемые к использованию.

Компоненты бывают двух видов в зависимости от метрик [3]: численные и категориальные. Численные компоненты могут визуализировать численные величины (рис. 2). Таким образом, два объекта визуализации можно сравнить между собой. Например, „во сколько раз один треугольник больше другого?“. Категориальные компоненты не могут этого делать. Например, нельзя задать вопрос: „во сколько раз один объект более треугольный, чем второй?“, но они могут визуализировать категории: „сколько треугольников вы видите среди шаров?“. При этом численные компоненты могут визуализировать и категориальные метрики: „сколько треугольников среднего размера вы видите? “.

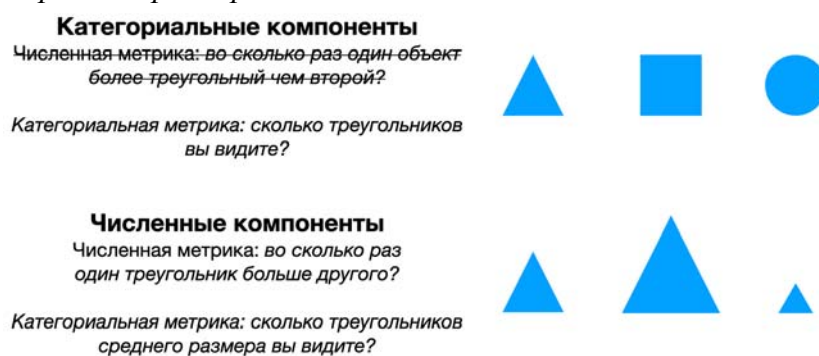


Рис. 2

Компоненты визуализации определены исходя их книги К. Леборга „Визуальная грамматика“ [4]. Были взяты только те компоненты, которые могут визуализировать метрики. В класс численных компонентов вошли: размер (объем в 3D), оттенок цвета, насыщенность цвета, прозрачность, кубическая система координат (СК), радиальная (цилиндрическая в 3D) система координат, вращение, масштабирование, движение; в класс категориальных — форма, основной цвет, текстура.

Очевидно, что эффективность визуализации численных и категориальных компонентов невозможно сравнить, так как при тестировании задаются разные типы вопросов. По этой причине было проведено два вида тестов (рис. 3).

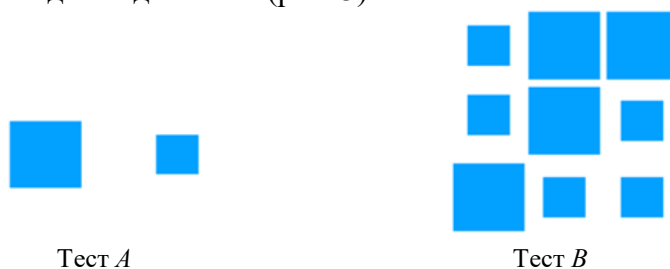


Рис. 3

Тест А — численный. Пользователю были представлены два объекта, которые идентичны друг другу во всем, кроме тестируемого компонента визуализации: например, два статичных куба одинакового размера, одинаковой формы, текстуры, прозрачности и насыщенности цвета. Затем один из компонентов изменялся. Было необходимо определить „во сколько раз первый объект более большой, прозрачный, синий, насыщенный, чем второй“.

Тест В — категориальный. Пользователю были представлены 32 объекта, которые идентичны друг другу во всем, кроме тестируемого компонента визуализации. Среди 32 объектов было выделено четыре категории. Например, 32 объекта с четырьмя разными формами.

Было необходимо определить „сколько вместе объектов X и Y “, где X и Y — треугольники, полосатые объекты, вращающиеся, синие и т. д.

Для каждого численного компонента проводились тесты A и B , для категориального — только B . Для каждого теста были созданы три различные комбинации, таким образом, для одного пользователя производилось три измерения степени восприятия одного компонента.

Тесты проводились в СПИИРАН с участием 20 человек — аспирантов СПИИРАН и студентов Санкт-Петербургского государственного университета коммуникаций М. А. Бонч-Бруевича. Тесты были реализованы в виде программы, написанной с использованием платформы Unity и запущенной в очках виртуальной реальности HTC vive.

Испытуемый проходил краткий инструктаж, как надевать и снимать шлем, как пользоваться контроллерами, как вводить ответ на виртуальной клавиатуре, как „хватать“ и отпускать виртуальные объекты, как перемещаться. После инструктажа испытуемый приступал к тестированию под наблюдением куратора в течение первых 6 заданий, при этом куратор лишь помогал освоиться с техникой и не вмешивался в ход эксперимента. Первые 6 заданий имитируют тестирование, для того чтобы испытуемый обучился работе с гарнитурой. Затем куратор удалялся, чтобы минимизировать влияние на испытуемого. В сумме испытуемый должен был пройти 63 задания (табл. 1).

Таблица 1

Компонент	Тип компонента	Количество тестов	
		A	B
—	Имитация тестирования	3	3
Размер	Численный	3	3
Оттенок цвета	Численный	3	3
Насыщенность цвета	Численный	3	3
Прозрачность	Численный	3	3
Вращение	Численный	3	3
Масштабирование	Численный	3	3
Движение	Численный	3	3
Форма	Категориальный	—	3
Основной цвет	Категориальный	—	3
Текстура	Категориальный	—	3
Кубическая СК	Численный	3	—
Радиальная СК	Численный	3	—

В среднем тестирование занимало 50 мин. Именно поэтому было принято решение ограничиться данным набором тестов, так как такое длительное время приводит к усталости испытуемых, что может сказаться на результатах тестирования.

В результате тестирования были получены распределения показателей точности и скорости интерпретации. На рис. 4, 5 показаны графики распределения показателей в виде box plot [5].

Точность была нормирована таким образом, что правильный ответ соответствовал отметке „0“. Изменение на единицу показывает отклонение в 100 % от правильного ответа. Например: правильный ответ равен 5 (на графике — 0), ответ пользователя равен 10 (на графике — 1) или 2,5 (на графике — 0,5).

В тесте A компоненты по точности интерпретации были разделены на 3 категории (рис. 4, a):

1) точные компоненты, верхний квантиль Q_3 которых меньше 1: движение, масштабирование, вращение и кубическая СК;

2) компоненты с погрешностями, верхний квантиль Q_3 которых больше 1 и меньше 2: радиальная СК, прозрачность и размер;

3) неточные компоненты, верхний квантиль Q_3 которых больше 2: оттенок, насыщенность.

В тесте *B* компоненты по точности интерпретации были также разделены на 3 категории (рис. 4, б):

- 1) точные компоненты, верхний квантиль Q3 которых равен 0: движение, масштабирование, вращение, цвет и форма;
- 2) компоненты с погрешностями, верхний квантиль Q3 которых меньше 1: размер, прозрачность и текстура;
- 3) неточные компоненты, верхний квантиль Q3 которых больше 1: оттенок, насыщенность.

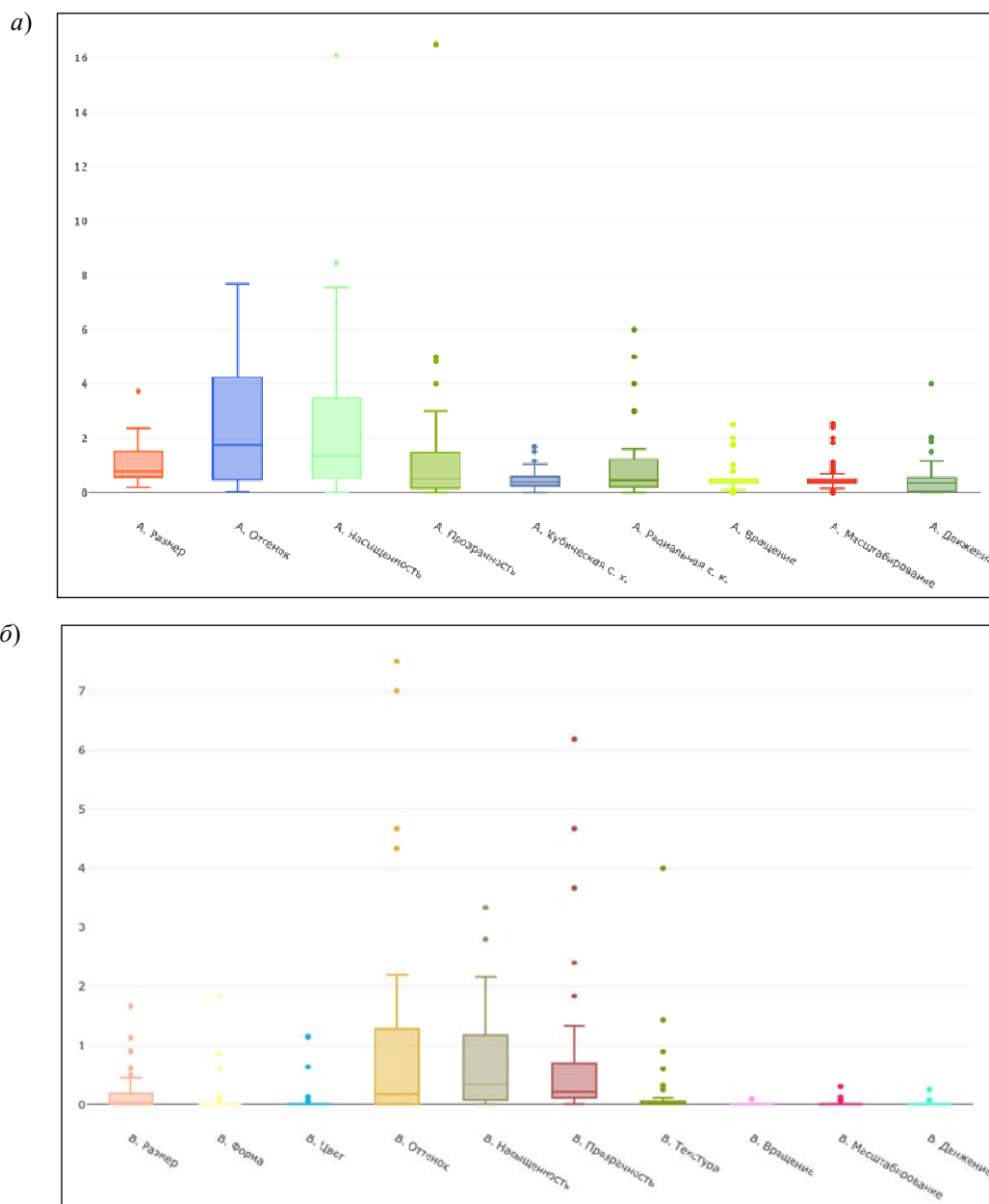


Рис. 4

Скорость принятия решений рассчитывалась как разность между временем начала теста (когда объекты появились перед пользователем) и временем его окончания (когда пользователь ввел ответ). На графиках время показано в секундах.

В тесте *A* компоненты по скорости интерпретации были разделены на 3 категории (рис. 5, а):

- 1) быстрые компоненты, верхний квантиль Q3 которых меньше 30 с: размер, насыщенность, прозрачность, масштабирование, движение;

2) приемлемые компоненты, верхний квантиль Q3 которых меньше 60 с: вращение, оттенок;

3) медленные компоненты, верхний квантиль Q3 которых больше 60 с: кубическая СК, радиальная СК.

В тесте *B* компоненты по скорости интерпретации также были разделены на 3 категории (рис. 5, б):

1) быстрые компоненты, верхний квантиль Q3 которых меньше 30 с: вращение, масштабирование, движение;

2) приемлемые компоненты, верхний квантиль Q3 которых меньше 60 с: размер, форма, цвет, насыщенность и текстура;

3) медленные компоненты, верхний квантиль Q3 которых больше 60 с: прозрачность, оттенок.

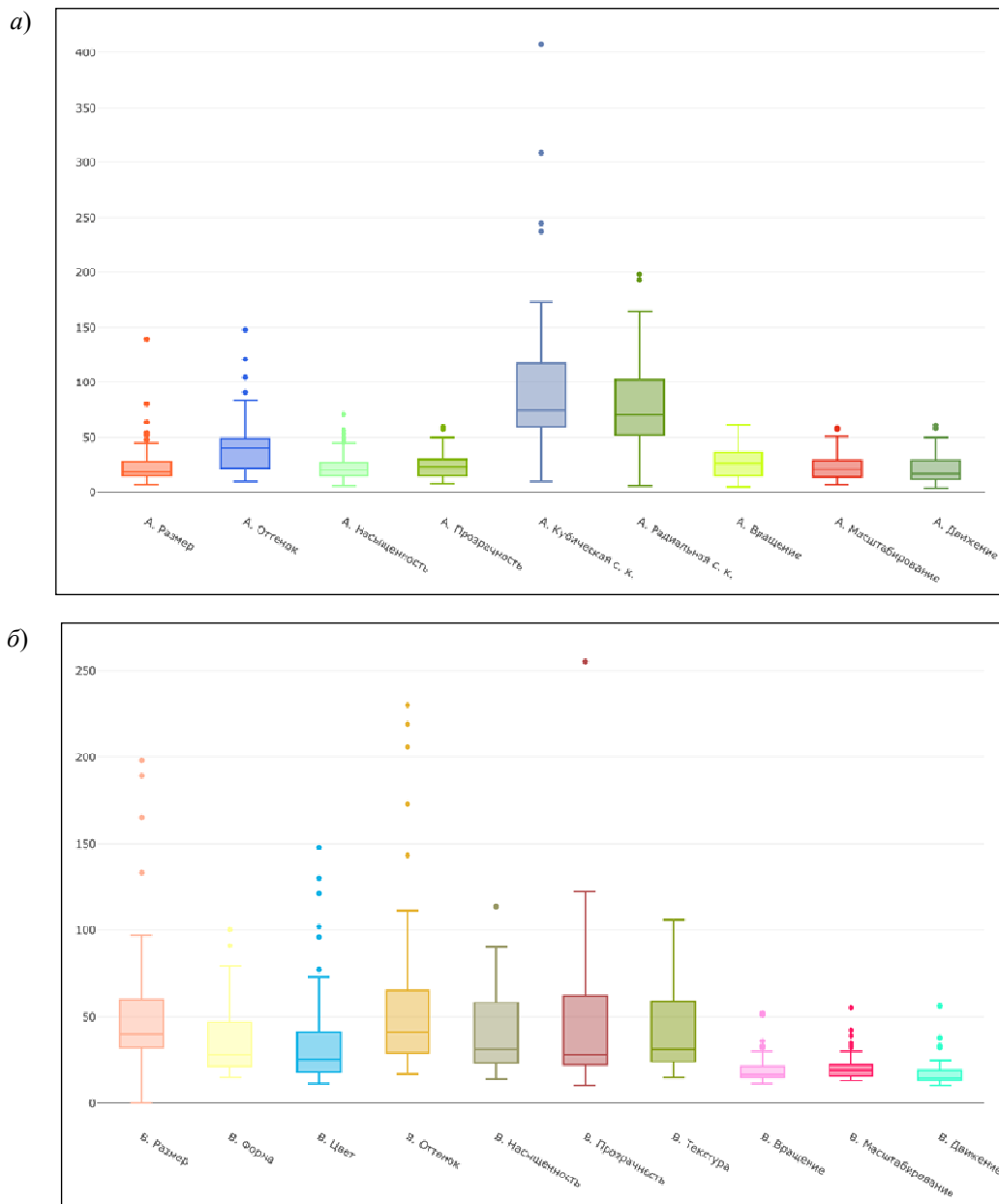


Рис. 5

Результаты тестирования сведены в табл. 2.

На основе точности и скорости интерпретации компонентов можно принимать решения при проектировании, чтобы максимизировать возможность получения эффективной модели визуализации.

Таблица 2

Компонент	Точность интерпретации		Скорость интерпретации	
	Тест А	Тест В	Тест А	Тест В
Размер	С погрешностями	С погрешностями	Быстрая	Приемлемая
Форма	—	Точная	—	Приемлемая
Основной цвет	—	Точная	—	Приемлемая
Отенок цвета	Неточная	Неточная	Приемлемая	Медленная
Насыщенность цвета	Неточная	Неточная	Быстрая	Приемлемая
Прозрачность	С погрешностями	С погрешностями	Быстрая	Медленная
Текстура	—	С погрешностями	—	Приемлемая
Кубическая СК	Точная	—	Медленная	—
Радиальная СК	С погрешностями	—	Медленная	—
Вращение	Точная	Точная	Приемлемая	Быстрая
Масштабирование	Точная	Точная	Быстрая	Быстрая
Движение	Точная	Точная	Быстрая	Быстрая

Пример прохождения теста и инструкции, которые выдавались испытуемым и наблюдателям, можно посмотреть по ссылке [6].

Работа выполнена при поддержке РФФИ, грант № 18-37-20047 мол_а_вед.

СПИСОК ЛИТЕРАТУРЫ

1. *Plaisant C.* The challenge of information visualization evaluation // Proc. of the Workshop on Advanced Visual Interfaces AVI. N. Y., USA: ACM Press, 2004. P. 109—116.
2. *Few S.* Save the pies for dessert // Visual Business Intelligence Newsletter. 2007, Aug. P. 1—14.
3. *Udina F.* Visualizing categorical data // J. of Statistical Software. 2004. N 11.
4. *Leborg C.* Visual Grammar: A Design Handbook (Visual Design Book for Designers, Book on Visual Communication). N. Y.: Princeton Arch. Press, 2006.
5. *Williamson D. F., Parker R. A., Kendrick J. S.* The box plot: A simple visual method to interpret data // Ann. of Internal Medicine. 1989. N 110(11). P. 916—921.
6. Пример прохождения теста и инструкции [Электронный ресурс]: <comsec.spb.ru/files/VR/index.html>, 08.07.2020.

Сведения об авторе

Максим Вадимович Коломеец — СПбФИЦ РАН, СПИИРАН, лаборатория проблем компьютерной безопасности; мл. научный сотрудник; E-mail: kolomeec@comsec.spb.ru

Поступила в редакцию
02.10.2020 г.

Ссылка для цитирования: Коломеец М. В. Эффективность визуализации данных в виртуальной реальности // Изв. вузов. Приборостроение. 2020. Т. 63, № 11. С. 1046—1052.

EFFECTIVENESS OF DATA VISUALIZATION IN VIRTUAL REALITY

M. V. Kolomeets

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

Results of experiments on testing the perception of 12 visualization components in virtual reality based on blind testing of 20 users, are presented. The tests are carried out using HTC Vive VR glasses

and controllers. An assessment of the speed and accuracy of visualization perception of 9 quantitative and 3 categorical components is performed. Based on the upper quantile of the distribution of estimates, the components recommended for use in visual analytics systems are determined. The obtained estimates of the speed and accuracy of perception allow to account for the features of perception when designing analytic systems using virtual reality.

Keywords: visual analytics, virtual reality, data analysis, assessment of perception effectiveness, blind testing

REFERENCES

1. Plaisant C. *Proceedings of the Workshop on Advanced Visual Interfaces AVI*, NY, USA, ACM Press, 2004, pp. 109–116.
2. Few S. *Vis. Bus. Intell. Newsl.*, 2007, pp. 1–14.
3. Udina F. *J. Stat. Softw.*, 2004, no. 11.
4. Leborg C. *Visual Grammar: A Design Handbook (Visual Design Book for Designers, Book on Visual Communication)*, 2006.
5. Williamson D.F., Parker R.A., Kendrick J.S. *Ann. Intern. Med.*, 1989, no. 11(110), pp. 916–921.
6. comsec.spb.ru/files/VR/index.html. (in Russ.)

Data on author

Maxim V. Kolomeets

— 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;
E-mail: kolomeec@comsec.spb.ru

For citation: Kolomeets M. V. Effectiveness of data visualization in virtual reality. *Journal of Instrument Engineering*. 2020. Vol. 63, N 11. P. 1046—1052 (in Russian).

DOI: 10.17586/0021-3454-2020-63-11-1046-1052