УДК 152.5 DOI 10.21685/2307-4205-2020-2-4

Н. А. Северцев, А. В. Бецков, И. В. Прокопьев

СИСТЕМНОЕ ПРЕДСТАВЛЕНИЕ МЕТОДОЛОГИИ БЕЗОПАСНОСТИ

N. A. Severtsev, A. V. Betskov, I. V. Prokop'ev

SYSTEM PRESENTATION OF SECURITY CONCEPT

Аннотация. Выбранный в статье подход с позиции системного анализа демонстрирует методологию создания теории безопасности с учетом воздействия субъекта на работу исследуемого объекта внутренних и внешних возмущений. Продемонстрированы в качественном виде показатели безопасности в пространстве состояний, а также методы построения схем формирования оценки безопасности на основе информации и деформации параметрической области безопасности при различных возмущениях. Данный подход применим для обоснования методологии безопасности робототехнических систем и аэромобильных комплексов, в том числе обладающих искусственным интеллектом.

Ключевые слова: системный анализ, робототехнические системы, аэромобильные комплексы, искусственный интеллект, обобщенное понятие опасности, оценка безопасности системы, показатель безопасности, модифицированная граница, многоальтернативность, бифуркационные изменения, деформация параметрической области безопасности.

Abstract. The approach chosen in the article, from the point of view of system analysis, demonstrates the methodology for creating a security theory taking into account the influence of the subject on the work of the object under study of internal and external disturbances. Safety indicators in the state space are demonstrated in a qualitative form, as well as methods for constructing schemes for forming a safety assessment based on information and deforming the parametric safety domain under various perturbations. This approach is applicable to substantiate the safety methodology of robotic systems and airmobile complexes, including those with artificial intelligence.

Keywords: system analysis, robotic systems, airmobile complexes, artificial intelligence, generalized concept of hazard, system safety assessment, safety indicator, modified boundary, multi-alternative, bifurcation changes, deformation of the parametric safety domain.

Многие ученые признают необходимость формирования единой терминологической и понятийной научной базы. Тем не менее приходится признать, что до сих пор терминологии обобщенной безопасности для различных отраслей науки и техники нет, особенно в формализованной постановке. Есть понятие безопасности систем для каждой отрасли научных знаний, хозяйствования и в философском понимании – вербальном представлении, которое трактуется применительно к какому-либо объекту (системе), принадлежащему той или иной отрасли. Данная статья посвящена обобщенному понятию опасности, независимо от принадлежности исследуемой системы (объекта). Своего рода унифицированный подход описания опасного или безопасного состояния на формализованной основе.

Пусть имеется система, на которую действуют внешние и внутренние возмущения при управлении данной системой. Весь спектр этих случайных воздействий может привести систему к разрушению. Задача состоит в том, чтобы построить оценки, позволяющие в процессе работы системы численно определить угрозу распада системы для своевременного принятия мер к недопущению этого. Очевидно, такая оценка должна быть построена на движении системы, т.е. представлять функционал, так как изменяющееся состояние системы может нести в себе информацию о приближении опасного порога функционирования системы.

Принципиальная схема формирования показателя безопасности J_6 на основе всех информационных потоков представляется следующим образом (рис. 1).

Например, увеличивающаяся амплитуда колебаний (качки) водного судна выше пределов устойчивости позволяет судить об угрозе его оверкиля, т.е. когда центр тяжести (центр масс) окажется выше центра величины, т.е. центра гидростатического давления. В этом примере катастрофа (оверкиль водного) будет являться результатом изменения его состояния, а не причины, его вызвавшей.

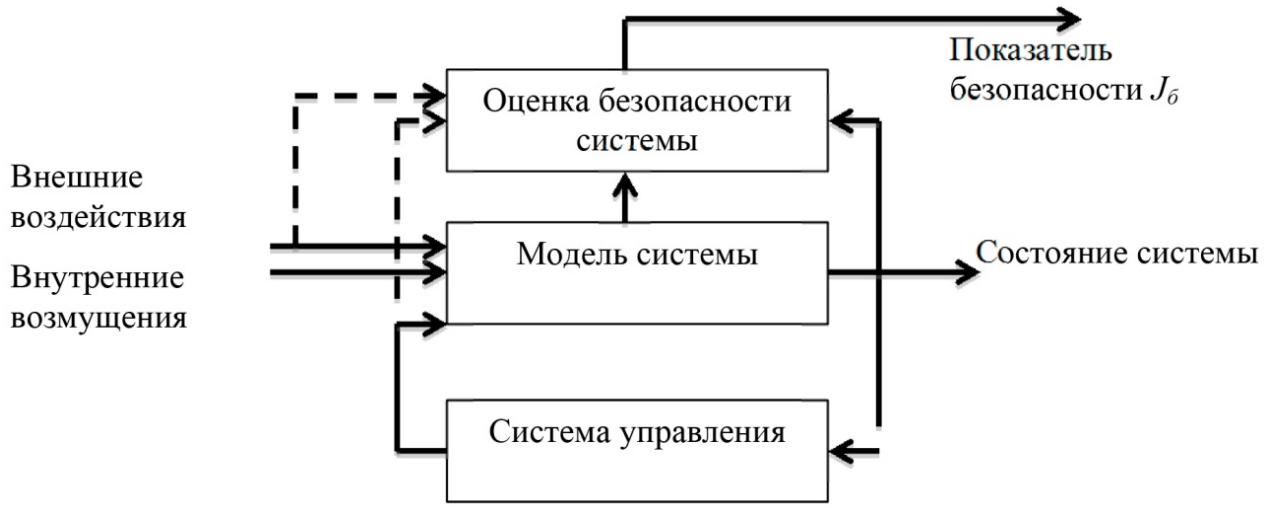

Рис. 1. Схема формирования оценки безопасности на основе информации

Следовательно, все пространство состояний системы можно разделить на две области: одна будет составлять множество опасных для существования системы состояний $C_о$, а другой будут принадлежать все безопасные состояния $C_б$. Объединение этих множеств опишет все возможные состояния системы ($C = C_о \cap C_б$). Надо выделить две противоречивые тенденции при построении $C_б$. С одной стороны, чтобы гарантировать безопасность системы из этого множества следует исключить все режимы, которые могли бы приводить к ее деструкции, что означает – множество надо сужать. Но ограничение допустимых состояний стесняет возможности функционирования, следовательно, уменьшает возможности достижения целевого множества. Преодоление противоречия осуществляется поиском компромисса. В этом случае следует искать в удалении от границы безопасности, т.е. уменьшать область безопасности – наличие некоторого запаса безопасности и предоставить ЛПР время на парирование угроз, а также повысить уровень защищенности. Такой подход можно определить следующим образом: объективную оценку безопасности системы можно произвести, наблюдая ее состояние. Для этого следует построить подмножество безопасных состояний, выделив все режимы, приводящие к разрушению (потере гомеостаза) системы. Строго говоря, область безопасности может быть сформирована на основе полномасштабного моделирования работы системы с управлением в реальных условиях и действия на нее всевозможных возмущений. Для сохранения гомеостаза системы необходимо создать запас безопасности, введение которого обеспечивает уменьшение области безопасности.

Однако даже если построена модифицированная граница области безопасности с учетом запаса $\Gamma_{бм}$, то находить в пространстве С кратчайшее расстояние от текущего состояния системы, задаваемого вектором С, до границы $\Gamma_{бм}$ представляется затруднительным.

Во-первых, наличие модифицированной области $C_{бм}$ в пространстве состояний наиболее объективно свидетельствует об удаленности текущего режима работы системы от состояния, угрожающего его целостности. Однако для повышения временного ресурса для устранения неполадок в системе, для увеличения оперативности и качества управления было бы желательно располагать информацией о причинах, обусловливающих приближение состояния системы к опасной границе. Для этого рассмотрим факторы, определяющие появление опасных для системы режимов, т.е. требуется сделать анализ угроз, проникающих через единственный канал – через воздействие на систему. Например, лучше сделать профилактику судна «Булгария», выяснить все причины неполадок и устранить их, чем выходить в плавание с этими не устраненными неполадками (а их было много), дожидаться оверкиля судна с большими жертвами.

Во-вторых, необходимо определить показатели безопасности, имеющие большую физическую наглядность и меньшую сложность вычислений, нежели определение в пространстве состояний расстояния до границы (рис. 2).

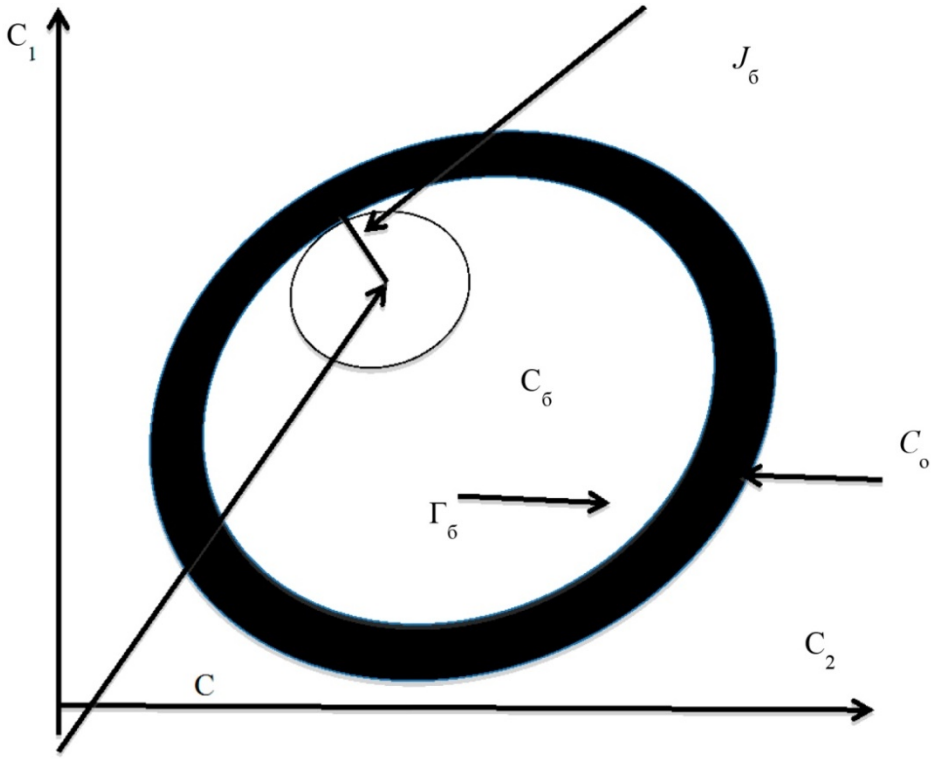

Рис. 2. Показатель безопасности в пространстве состояний

Решение первой задачи базируется на рис. 1. Если раньше область безопасности строилась на основе информации о состоянии (выход модели), то теперь следует привлекать сведения о входных воздействиях, т.е. использовать каналы, изображенные пунктирными линиями. Это воздействия управления, внешние и внутренние воздействия. Подробный разбор этих воздействий – это отдельные темы. Однако мы их изложим в кратком и основополагающем представлении. Итак, внутренние возмущения включают в себя изменения каналов передачи информации (структурные трансформации) и отклонения параметров от номинальных значений (параметрические возмущения). Неожиданная реорганизация структуры является самой опасной, так как особенно сильно влияет на динамическое состояние системы. Предвидеть подобные преобразования в самоорганизующихся системах весьма сложно в силу их многоальтернативности и малой предсказуемости; такая задача имеет характер бифуркационных изменений. В искусственно созданных системах структура мало подвержена внезапным преобразованиям, так как они есть результат синтеза системы, воплощенного в реальность совокупностью технических решений, направленных именно на поддержание целостности системы. Что касается управлений как целенаправленных воздействий на динамику системы, то в искусственных системах они идентифицируются просто. В естественных системах понятие управления часто размыто. Тогда напрашивается вывод о том, что основную проблему при построении оценки безопасности доставляют параметрические возмущения и внешние воздействия среды. Итак, будем исходить из предположения, что область безопасности $C_{бм}$ построена. Тогда задача заключается в пересчете этого подпространства пространства состояний в пространство входных воздействий – параметрических $C^{п}_{бм}$ и внешних $C^{в}_{бм}$ возмущений. Однако такое решение затруднительно, так как из реакций системы трудно выделить их причинную обусловленность, т.е. установить вклад каждого возмущения в результат – состояние. Поэтому приходится обойтись без процедуры общего пересчета, а по отдельности строить области для каждого входного воздействия. Методически это заключается в нахождении соответствия границы $Г_{бм}$ множества $C_{бм}$ границам в пространствах параметров и воздействия внешней среды, соответственно $Г^{в}_{бм}$ и $Г^{п}_{бм}$. Перебирается весь спектр воздействий, например методом Монте-Карло, и находится реакция системы на каждый входной сигнал. Те сигналы, которые приводят к распаду системы, и признаются опасными.

Сложность процедуры усугубляется еще одним обстоятельством: в общем случае динамических нелинейных систем существует взаимная корреляционная зависимость области нормального

функционирования системы от параметрических и внешних возмущений. Грубо говоря, для каждого уровня внешних воздействий имеется свое множество допустимых значений параметров системы (рис. 3).

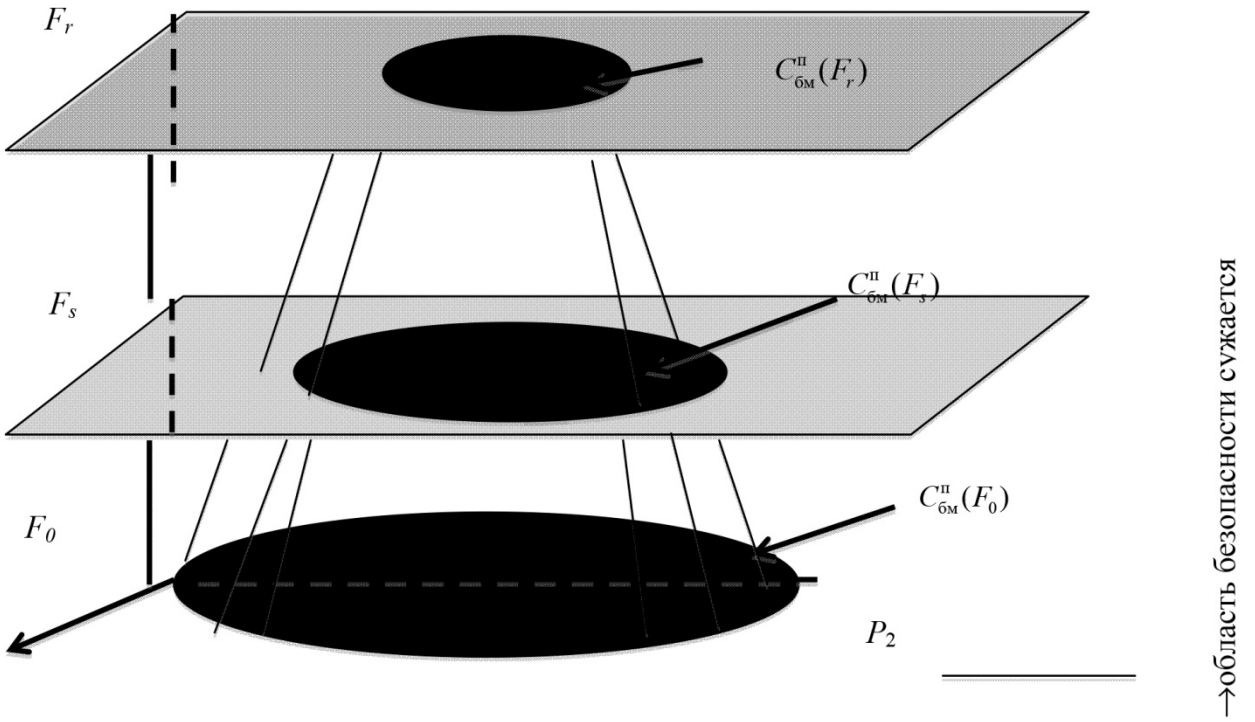

Рис. 3. Деформация параметрической области безопасности при различных возмущениях

Горизонтальная плоскость (рис. 3) есть множество параметров $P = \{P_i\}$, $i = 1, 2$, где выделена область безопасности $C^{\text{п}}_{\text{бм}}$. По ординате отложена величина уровня внешних возмущений F с тремя координатами-воздействиями F_0, F_s, F_r. Для разных уровней возмущений область $C^{\text{п}}_{\text{бм}}$ меняется, т.е. становится их функцией. Можно предположить, что по мере роста воздействий на систему параметрическая область безопасности сужается. Таким образом, в результате построений мы располагаем двумя наборами взаимосвязанных множеств: областями безопасности $C^{\text{в}}_{\text{бм}}$ и $C^{\text{п}}_{\text{бм}}$, построенными в пространстве входных воздействий и флуктуирующих параметров соответственно. Тем самым при оценке безопасности можно перейти от изучения состояний системы к наблюдению за выходными сигналами, а значит, заменить анализ следствия анализом причин. Обращение непосредственно к угрозам, исходящим от среды и нарушений в системе привело к размножению областей безопасности. Вместо итоговой области в пространстве состояний мы вынуждены иметь дело с несколькими областями по числу каналов проникновения угроз в систему, да к тому же области связаны функционально. Конечно, это делает алгоритмы обеспечения безопасности более сложными.

Мы рассмотрели решение первой задачи. Теперь перейдем ко второй.

1. Нарушение устойчивости системы означает появление в ней расходящихся процессов, которые не поддаются управлению и немедленно приводят к дезинтеграции системы. Существует общий подход к исследованию устойчивости на результатах А. М. Ляпунова, от которого трудно ожидать непосредственной применимости к проблеме безопасности в силу отсутствия возможности получения конкретных оценок. Развитие метода показало, что его эффективное использование требует разбиения общей задачи на классы, а наиболее продвинутыми оказались решения частных задач с вполне конкретными видами нелинейностей.

Нарушение устойчивости не столь очевидно, но имеет губительные последствия. Поэтому при определении безопасности режимов работы системы следует уделять внимание и устойчивости. Тогда границы $\Gamma^{\text{в}}_{\text{б}}$ и $\Gamma^{\text{п}}_{\text{б}}$ областей безопасности будут описывать нарушение условий устойчивости системы при превышении уровня допустимых внешних воздействий и запредельном отклонении па-

раметров системы. Мера безопасности как гарантия устойчивости определяется посредством оценки удаления текущего состояния системы от границы, описывающей переход в неустойчивое состояние (рис. 2). Однако в настоящее время не существует общих методов построения областей устойчивости в пространствах воздействий и параметров, которые были бы адекватными областями безопасности. Это обстоятельство ставит под сомнение возможность разработки общей конструктивной теории безопасности, по крайней мере, при современном уровне теории устойчивости в безопасности функционирования системы. Выход из указанного затруднения лежит на пути декомпозиции проблемы, разбиения общей задачи на ряд частных. Иначе, если не удается построить теорию безопасности для всех типов систем, то необходимо решать задачи для систем отдельных классов или в худшем случае ограничиться отысканием частных решений для конкретного вида систем, оценка устойчивости которых известна. Действительно, при изучении системы на безопасность, всегда можно выстроить приоритеты факторов по их влиянию на ее безопасность. Тогда в последующих исследованиях устойчивости можно принимать во внимание только наиболее критичные, для которых и вычислять области допустимых значений.

2. Управляемость системы по своей содержательности сходна с понятием области достижимости. Оба характеризуют достижение цели. Для линейных систем условие управляемости известно. Для нелинейных систем это условие сопряжено с большими трудностями. С практической точки зрения достижение цели требует:

а) того, чтобы управляющие органы могли воздействовать на параметры состояния, в которых фиксируется цель;

б) того, чтобы было достаточно ресурсов для движения по траектории, проходящей через цель. Эти соображения имеют ясную физическую наглядность, что позволяет выполнить их при создании системы;

в) требование наблюдаемости системы состоит в доступности измерений степеней свободы, информация о которых необходима для управления системой. Выполнение этого требования на практике осуществляется путем создания измерителей, достаточных для идентификации состояний и управления движением системы;

г) ресурсное обеспечение обычно удовлетворяется на стадии проектирования или подготовки системы к выполнению конкретной задачи. Повышение их порогового значения приводит к ухудшению экономических показателей. Однако таким ущербом можно пренебречь по сравнению с угрозой разрушения системы, поэтому на него идут сознательно.

Заключение

1. Для построения оперативной системы мер по недопущению превращения угроз в катастрофические (аварийные) для системы целесообразно использовать информацию о входных воздействиях со стороны среды и отклонениях параметров системы. Это позволяет подвергнуть анализу не следствия (опасные изменения состояния), а причины появления угрожающих состояний. Однако такой путь связан с усложнением системы, как в алгоритмическом смысле, так и информационном – требуются сведения об угрозах существованию системы. Можно ожидать, что объединение информационных потоков о состоянии, системах и причинах его изменения даст наилучшие результаты, как позиций простоты реализации, так и эффективности системы обеспечения безопасности.

2. Из числа доступных анализу характеристик динамики системы пригодны для оценки безопасности показатели управляемости, наблюдаемости и устойчивости, а также энергетические ресурсы. Большинство из них достаточно просто удовлетворяется при проектировании или подготовке системы к работе, поэтому их можно не учитывать при анализе безопасности системы. Исключением можно считать устойчивость, оценка которой изменяется при воздействиях со стороны внешней среды и внутренних возмущениях. Эту характеристику следует использовать при построении области безопасности.

3. Применение оценки устойчивости в качестве показателя безопасности в общем случае затруднительно, что приводит к необходимости подвергать анализу на безопасность отдельные классы или только конкретные системы. Для построения области безопасности по критерию устойчивости и ее использования при контроле целесообразно применять упрощение модели системы. Упрощение рационально проводить путем выявления критических угроз и/или их объединения

в эталонные группы; отказа от непрерывной модели системы и перехода к конечным зависимостям между воздействиями и реакциями системы.

Библиографический список

1. *Могилевский, В. Д.* Основы теории систем : в 2 ч. / В. Д. Могилевский. – Москва : МИРЭА, 1997. – Ч. 1. Проблемы формализации динамических систем. – 75 с. ; Ч. 2. Гамильтоново представление движения систем. – 115 с.
2. *Северцев, Н. А*. Введение в безопасность / Н. А. Северцев, А. В. Бецков. – Москва : ВЦ РАН им. А. А. Дородницына, 2018. – 176 с.
3. *Северцев, Н. А*. Системный анализ теории безопасности / Н. А. Северцев, А. В. Бецков. – Москва : МГУ им. М. В. Ломоносова, 2018. – 452 с.

References

1. Mogilevskiy V. D. *Osnovy teorii sistem: v 2 ch.* [Fundamentals of systems theory: in 2 parts]. Moscow: MIREA, 1997, part 1, 75 p.; part 2, 115 p. [In Russian]
2. Severtsev N. A., Betskov A. V. *Vvedenie v bezopasnost'* [Introduction to security]. Moscow: VTs RAN im. A. A. Dorodnitsyna, 2018, 176 p. [In Russian]
3. Severtsev N. A., Betskov A. V. *Sistemnyy analiz teorii bezopasnosti* [A systematic analysis of the theory of security]. Moscow: MGU im. M. V. Lomonosova, 2018, 452 p. [In Russian]

Северцев Николай Алексеевич
доктор технических наук, профессор,
главный научный сотрудник,
отдел управления робототехническими устройствами,
Федеральный исследовательский центр «Информатика и управление» Российской академии наук
(Вычислительный центр им. А. А. Дородницына РАН)
(Россия, г. Москва, ул. Вавилова, 40)
E-mail: severs@ccas.ru

Severtsev Nikolay Alekseevich
doctor of technical sciences, professor,
chief researcher,
department of robotic systems management devices,
Federal research center «Computer science and control» of RAS
(Dorodnitsyn computer center of the Russian Academy of Sciences)
(40 Vavilova street, Moscow, Russia)

Бецков Александр Викторович
доктор технических наук, доцент,
заместитель начальника,
Академия управления МВД России
(Россия, г. Москва, ул. Зои и Александра Космодемьянских, 8)
E-mail: abckov@mail.ru

Betskov Aleksandr Viktorovich
doctor of technical sciences, associate professor,
deputy chief,
Russian Academy of the Interior Ministry
(8 Zoi i Aleksandra Kosmodem'yanskikh street, Moscow, Russia)

Прокопьев Игорь Витальевич
доктор технических наук,
ведущий научный сотрудник,
Федеральный исследовательский центр «Информатика и управление» Российской академии наук
(Вычислительный центр им. А. А. Дородницына РАН)
(Россия, г. Москва, ул. Вавилова, 40)
E-mail: fvi2014@list.ru

Prokop'ev Igor' Vital'evich
doctor of technical sciences, leading researcher,
Federal research center «Computer science and control» of RAS
(Dorodnitsyn computer center of the Russian Academy of Sciences)
(40 Vavilova street, Moscow, Russia)

Образец цитирования:

Северцев, Н. А. Системное представление методологии безопасности / Н. А. Северцев, А. В. Бецков, И. В. Прокопьев // Надежность и качество сложных систем. – 2020. – № 2 (30). – С. 26–31. – DOI 10.21685/2307-4205-2020-2-4.