О МОДЕЛЯХ И МЕТОДАХ ВЕРОЯТНОСТНОГО АНАЛИЗА ЗАЩИТЫ ИНФОРМАЦИИ В СТАНДАРТИЗОВАННЫХ ПРОЦЕССАХ СИСТЕМНОЙ ИНЖЕНЕРИИ

Костогрызов А.И.[1]

Цели: *обоснование и описание методического аппарата системной инженерии в части прогнозирования рисков с учетом требований по защите информации.*

Методы исследования включают: *методы теории вероятностей, риск-ориентированные модели для прогностического анализа стандартизованных процессов системной инженерии.*

Результат: *описаны взаимоувязанные модели и методы, систематизированные для использования при планировании и реализации стандартизованных процессов системной инженерии. Их применение позволяет осуществлять анализ влияния защищенности информации в терминах прогнозируемых рисков. Методы и модели реализованы в комплексе стандартов системной инженерии и аналитически поддерживают эффективную реализацию процессов соглашения, организационного обеспечения проекта, технического управления и технических процессов по ГОСТ Р 57193 (ISO/IEC/IEEE 15288) применительно к системам различного назначения (всего 30 процессов). Предложенные модели и методы системного анализа защиты информации в стандартизованных процессах системной инженерии развивают сложившиеся подходы к прогнозированию рисков, обеспечению и повышению безопасности систем. Использование предложенных моделей и методов в жизненном цикле систем способствует выявлению «узких мест», обоснованию способов снижения рисков в реализуемых стандартизованных процессах с учетом требований по защите информации, поддерживает принятие решений в аналитических задачах системной инженерии.*

Научная новизна: *предложенный методический аппарат развивает сложившиеся подходы к прогнозированию рисков, обеспечению и повышению безопасности систем. Идеи реализованы в национальных стандартах ГОСТ Р 59329 – ГОСТ Р 59357. Они позволяют предприятиям перейти к прагматичному внедрению риск-ориентированного подхода с использованием аналитических возможностей решения обратных задач эффективного управления безопасностью, исходя из задаваемого уровня допустимого риска.*

Ключевые слова: *риск-ориентированный подход, вероятностные модели, информационная безопасность, прогнозирование рисков, стандарты системной инженерии, системный анализ.*

DOI:10.21681/2311-3456-2022-6-71-82

1. Введение

В условиях неопределенностей для решения прикладных задач системной инженерии широкое распространение на практике получил риск-ориентированный подход. Международные стандарты содержат в основном положения, ориентирующие главным образом на качественные показатели рисков без методических рекомендаций того, как оценивать риски количественно на научной основе (а не на субъективных мнениях) в условиях предпринимаемых мер по противодействию различного рода угрозам – см., например, ГОСТ Р ИСО/МЭК 27005 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Недостаток приемлемых моделей и методов системной инженерии означает невозможность корректного аналитического решения обратных задач управления безопасностью исходя из задаваемого уровня допустимого риска. Этим обусловлена актуальность тематики исследований.

В последние годы построение стандартов по защите информации осуществляется в увязке со стандартизованными процессами жизненного цикла систем. К таковым относятся 30 основных процессов – процессы соглашения (приобретения и поставки продукции и услуг для системы), организационного обеспечения проекта (процессы управления моделью жизненного цикла, инфраструктурой, портфелем проектов, человеческими ресурсами, качеством, знаниями), технического

1 Костогрызов Андрей Иванович, заслуженный деятель науки РФ, доктор технических наук, профессор, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, г. Москва, Россия. E-mail: Akostogr@gmail.com

управления (процессы планирования проекта, оценки и контроля проекта, управления решениями, управления рисками, управления конфигурацией, информацией, измерений, гарантии качества) и технических процессы (анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы) – см. ГОСТ Р 57193–2016 «Системная и программная инженерия. Процессы жизненного цикла систем». Перечисленные стандартизованные процессы в полной мере характеризуют цели и выполняемые действия в жизненном цикле различного рода систем, к которым, в частности, относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, транспорта, связи, энергетики, банковской сфере, топливно-энергетического комплекса, горнодобывающей, металлургической и химической промышленности и др. Учитывая, что для многих критически важных систем потенциальные ущербы и затраты на ликвидацию последствий нарушений безопасности в условиях разнородных угроз могут на порядок превышать затраты на превентивные меры, необходим поиск эффективных решений для противодействия угрозам и обеспечения эффективного управления рисками.

В целом настоящая работа посвящена методическому обзору подходов к решению задач системного анализа для использования при планировании и реализации стандартизованных процессов системной инженерии. Для реализуемых процессов предлагаемые решения направлены на выявление «узких мест», обоснование способов снижения рисков и их удержание в допустимых пределах с учетом требований по защите информации. Предлагаемые вероятностные модели и методы развивают сложившиеся вероятностные подходы [1-12] и доведены до уровня реализации в ГОСТ Р 59329 – ГОСТ Р 59357. Они применимы там, где имеет место повторяемость событий. Их имеет смысл применять в сравнении или в комбинации или в дополнение к существующим методам. Там, где часто требуется прогнозный анализ или где используемые подходы оказываются малоэффективными, предлагаемые модели и методы могут быть использованы как рациональная альтернатива в дополнение к ранее применявшимся методам.

2. Общие положения

Научный взгляд на процессы возникновения и реализации разнородных угроз и системное отображении реальных и возможных событий на временную ось характеризуются частотой возникновения угроз, временем их развития и системными (или нередко на практике системно не обоснованными) мерами и технологиями противодействия угрозам.

Для эффективного управления используется логический переход от частных выводов, сделанных для конкретных систем, к более общим выводам относительно сложных систем и их элементов, получаемых вне зависимости от их функционального назначения по результатам вероятностного моделирования. Предлагаемые идеи, модели, методы и технологии рассчитаны на использование обратной связи для решения задач обоснования требований и условий, гарантирующих непревышение задаваемых допустимых рисков.

Как частное – рассматриваются конкретные системы и отдельные их составные элементы, функционирующие в конкретных условиях. Прогностическая обработка данных мониторинга для противодействия угрозам и обеспечения эффективного управления для таких систем рассмотрена в статье на многочисленных примерах.

Как общее – предлагается логический переход к сложным системам, допускающий декомпозицию систем для решения практических задач в терминах вероятности «успеха» («отсутствия нарушений функциональной целостности») или «неудачи» («нарушений *функциональной целостности») в течение прогнозного периода времени*. При этом под *функциональной* целостностью системы (элемента) понимается такое ее (его) состояние, при котором обеспечивается достижение целей ее (его) функционирования.

Предлагается осуществлять вероятностное прогнозирование развития случайных процессов во времени с тем, чтобы не только действовать согласно прогнозу, но и сравнивать прогнозы и их совпадения с последующими реалиями, накапливать и использовать эти знания. Именно в накоплении, анализе и использовании появляющихся знаний о возможной *функциональной* целостности системы в будущем заключается когнитивность решений задач прогностической обработки данных мониторинга.

При функционировании интересуемой системы в условиях складывающихся разнородных угроз степень приемлемости происходящих событий *предлагается оценивать вероятностью «успеха» и/или* «неудачи» (ри-

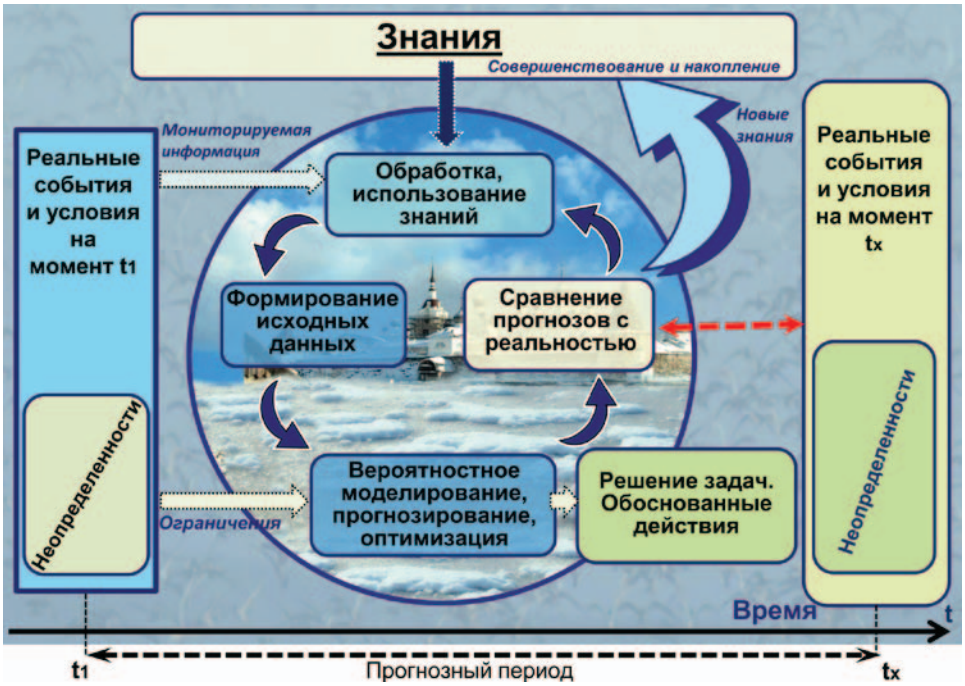

Рис. 1. Суть предлагаемого когнитивного решения задач системного анализа

ском «неудачи» с учетом последствий) в течение заданного прогнозного периода времени. При этом прогнозный период времени должен задаваться таким, чтобы за это время успеть восстановить возможности, которые могут оказаться утраченными, или осуществить предстоящее действие, с которым была связана инициация решения задачи. Такое поведение означает функционирование в реальном времени.

В каждом конкретном случае моделирования понятие «успеха» должно быть определено в терминах приемлемого состояния интересуемой системы для выполнения заданных или ожидаемых функций. Понятие «неудачи» означает отсутствие «успеха». В общем случае под *«успешностью»* функционирования интересуемой системы в течение заданного прогнозного периода времени понимается сохранение приемлемого уровня качества, безопасности или эффективности функционирования системы для выполнения ее заданных или ожидаемых функций. Соответственно «неудача» для интересуемой системы означает наступление неприемлемого уровня качества, безопасности или эффективности ее функционирования в течение заданного прогнозного периода времени. Под риском «неудачи» понимается вероятностная мера «неудачи» с возможными последствиями.

Суть предлагаемого когнитивного решения задач системного анализа и использования появляющихся знаний отражена на рис. 1. При этом возможные неопределенности для заданного периода прогноза (с начальной точки t_1 до момента t_x в будущем) могут быть учтены с использованием излагаемых ниже подходов к моделированию, прогнозированию и оптимизации.

Аналитическое прогнозирование рисков предлагается осуществлять на основе вероятностного моделирования систем. Для практического применения рекомендуются методы и модели [1-12] (далеко не исчерпывающие список адекватных моделей), где субъективные весовые коэффициенты исключены. Последнее – важно, т.к. продолжают широко применяться методы, базирующиеся на экспертных оценках, в т.ч. с использованием различного рода субъективно назначаемых коэффициентов. Экспертные коэффициенты еще как-то воспринималось на заре системного анализа, но сегодня их искусственное назначение может оказаться тормозом в современной науке, поскольку «эксперты» бывают разные. Человек в состоянии обозреть единицы-десятки элементов с отслеживаемыми параметрами, но не сотни-тысячи и более в их многочисленных взаимосвязях. Из-за субъективизма возможны «подгонки» под любые пожелания, ожидания и нормативы, не привязанные к конкретным методам. Вместе с тем, эти методы получают перспективное развитие с применением методов искусственного интеллекта и нечеткой логики – см., например [13-18].

Доведение предлагаемых моделей и методов до уровня рекомендуемых в национальных стандартах ГОСТ Р 59329 – ГОСТ Р 59357 позволяет предпри-

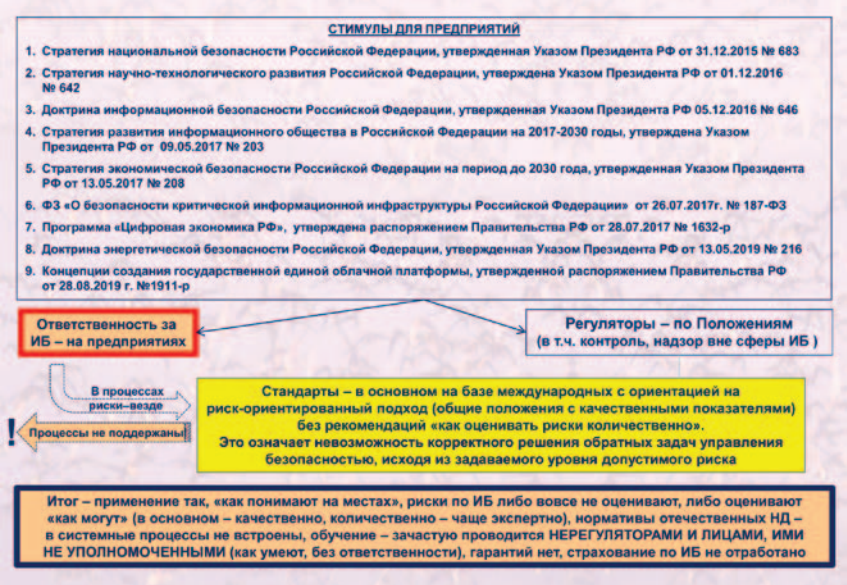

Рис. 2. Устаревший подход без количественного прогнозирования рисков в стандартизованных процессах системной инженерии

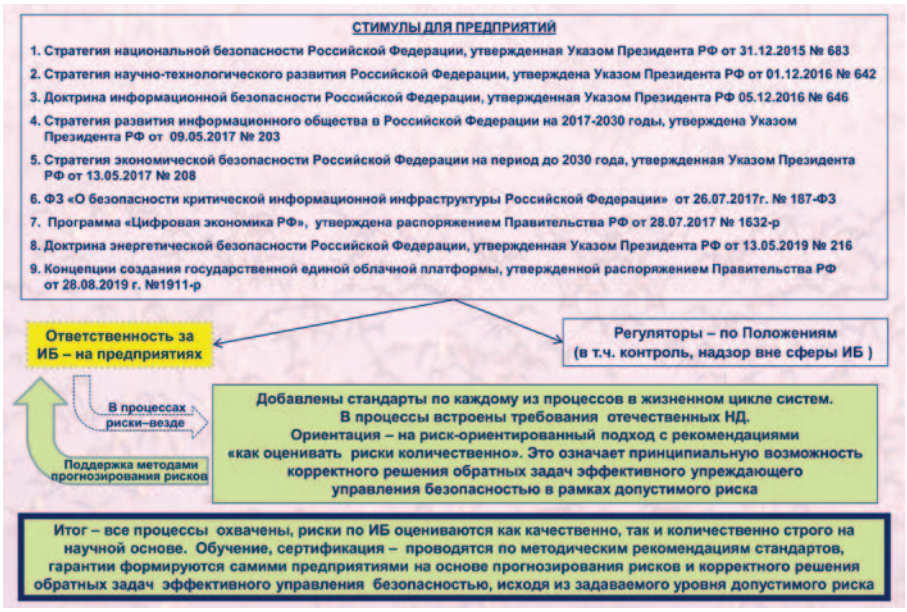

Рис. 3. Предлагаемый подход аналитической поддержки предприятий методами вероятностного прогнозирования рисков в стандартизованных процессах

ятиям при сохранении ответственности за обеспечение информационной безопасности (ИБ) перейти от использования рисков «как их понимают на местах» (в основном по качественным показателям) к охвату всех стандартизованных процессов методами количественного прогнозирования рисков. Это позволяет решать обратные задачи эффективного управления рисками, исходя из задаваемого уровня допустимого риска – см. рис. 2 и 3.

Предлагаемые модели базируются на классически построенном вероятностном пространстве (Ω, B, P), где Ω – конечное пространство элементарных событий; B – класс всех подмножеств множества Ω, удовлетворяющий свойствам сигма-алгебры; P – вероятностная мера на пространстве элементарных событий. При этом, поскольку пространство $\Omega=\{\omega_k\}$ – конечное, в моделях установлено отображение $\Omega_k \rightarrow p_k = P(\Omega_k)$ такое, что $p_k \geq 0$ и $\sum_k p_k = 1$. В условиях разнородных угроз уровень прогнозируемого качества или эффективности функционирования системы предлагается оценивать вероятностью «успеха», а прогнозируемой безопасности – вероятностью «неудачи» в течение заданного периода времени для составных компонентов и системы

в целом. При идентичных последствиях вероятность «неудачи» характеризует риск «неудачи». Само понятие приемлемого уровня функциональной целостности (в т.ч. «успешности») должно быть определено в терминах штатного состояния системы или составных элементов. Для детального анализа и решения прикладных задач применительно к каждому из элементов и подсистем сложная система декомпозируется до составных элементов. А для интегрального анализа модели сворачивая в модель системы (как единое целое).

Каждый из элементов представляется в виде «черного ящика», и для него могут быть применены различные вероятностные модели для расчетов и построения искомой функции распределения (ФР) времени между соседними нарушениями целостности, учитывающие разнородные угрозы, предпринимаемые меры контроля, мониторинга и восстановления целостности. Научный взгляд на процессы реализации разнородных угроз и системное отображение событий на временную ось характеризуется частотой возникновения угроз, временем их развития и применяемыми мерами и технологиями противодействия угрозам.

В случайных событиях присутствуют скрытые закономерности. Современный уровень развития теории вероятностей и теории случайных процессов независимо от природы разнородных угроз способен сформировать теоретическую и практическую базу прогнозирования функциональной целостности интересуемой системы во времени (в т.ч. для прогнозирования риска) и решения связанных с этим задач выработки и обоснования эффективных упреждающих мер. Фокусирование внимания именно на случайности событий позволяет использовать для их описания лишь характеристики времени (среднего времени или частоты наступления событий), безразмерные или стоимостные дополнительные характеристики, свойственные для объектов и систем различных приложений. Степень достижения ожидаемых результатов оценивается вероятностными показателями (например, с помощью вероятности безотказного функционирования, риска отказа или риска нарушения безопасности в течение заданного времени), рассчитываемыми с использованием применимых вероятностных моделей. Ниже приводятся рекомендуемые количественные показатели для системного анализа стандартизованных процессов с учетом требований по защите информации.

3. Примеры количественных показателей для прогнозирования рисков

Стандартизованные процессы, типовые действия и примеры показателей рисков отражены в табл. 1.

Более подробно предлагаемые показатели, например, в приложении к системам дистанционного контроля в опасном производстве раскрыты в ГОСТ Р 58494 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов», см. также [4].

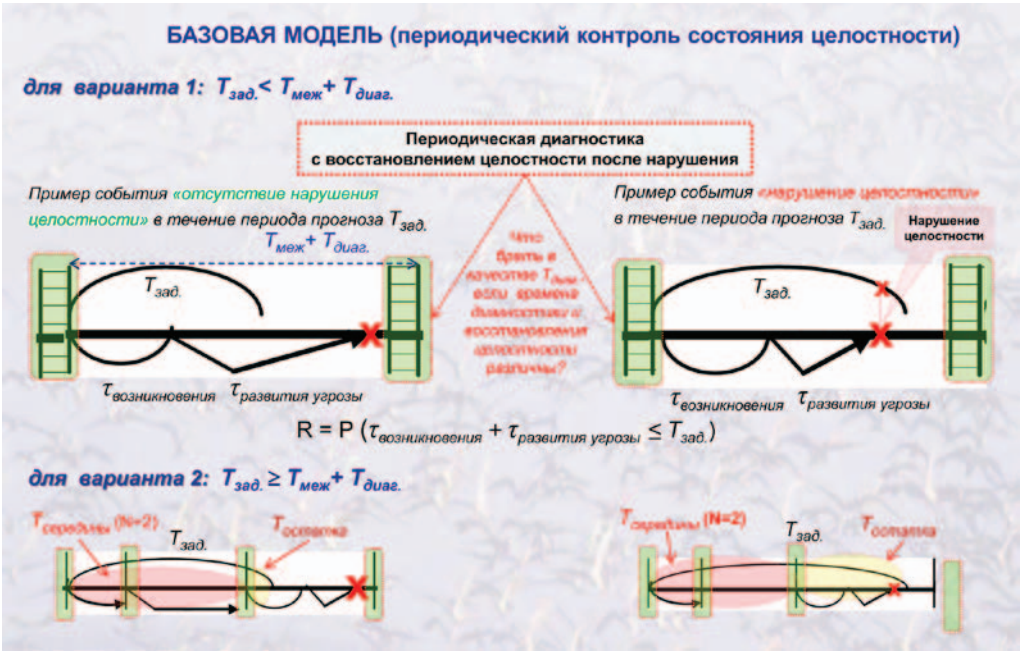

Рис. 4. Формальные случаи сохранения и нарушения целостности

Таблица 1

Стандартизованные процессы, типовые действия и примеры показателей рисков

Стандартные процессы по ГОСТ Р 57193	**Защищаемые ресурсы и действия в процессе**	**Примеры показателей рисков (по ГОСТ Р 59329 –ГОСТ Р 59357)**
Процесс приобретения продукции и/или услуг для системы	См. подробнее ГОСТ Р 59329	1) риск нарушения надежности реализации процесса без учета требований по защите информации; 2) риск нарушения требований по защите информации в процессе; 3) интегральный риск нарушения реализации процесса с учетом требований по защите информации
Процесс поставки продукции и услуг для системы	См. ГОСТ Р 59329	То же
Процесс управления моделью жизненного цикла системы	См. ГОСТ Р 59330	То же
Процесс управления инфраструктурой системы	См. ГОСТ Р 59331	То же
Процесс управления портфелем проектов	См. ГОСТ Р 59332	То же
Процесс управления человеческими ресурсами системы	См. ГОСТ Р 59333	То же
Процесс управления качеством системы	См. ГОСТ Р 59334	То же
Процесс управления знаниями о системе	См. ГОСТ Р 59335	То же
Процесс планирования проекта	См. ГОСТ Р 59336	То же
Процесс оценки и контроля проекта	См. ГОСТ Р 59337	По ГОСТ Р 59337 для всех процессов
Процесс управления решениями	См. ГОСТ Р 59338	То же, что для процесса приобретения продукции и/или услуг для системы
Процесс управления рисками для системы	См. ГОСТ Р 59339	По ГОСТ Р 59339 для всех процессов
Процесс управления конфигурацией системы	См. ГОСТ Р 59340	То же, что для процесса приобретения продукции и/или услуг для системы
Процесс управления информацией системы	См. ГОСТ Р 59341	1) вероятностные показатели, характеризующие надежность и своевременность представления, полноту, достоверность и конфиденциальность используемой информации; 2) риск нарушения надежности реализации процесса без учета требований по защите информации; 3) риск нарушения требований по защите информации в процессе; 4) интегральный риск нарушения реализации процесса с учетом требований по защите информации
Процесс измерений системы	См. ГОСТ Р 59342	То же, что для процесса приобретения продукции и/или услуг для системы
Процесс гарантии качества для системы	См. ГОСТ Р 59343	По ГОСТ Р 59343 для всех процессов

Стандартные процессы по ГОСТ Р 57193	Защищаемые ресурсы и действия в процессе	Примеры показателей рисков (по ГОСТ Р 59329 –ГОСТ Р 59357)
Процесс анализа бизнеса или назначения системы	См. ГОСТ Р 59344	То же, что для процесса приобретения продукции и/или услуг для системы
Процесс определения потребностей и требований заинтересованной стороны	См. ГОСТ Р 59345	То же
Процесс определения системных требований	См. ГОСТ Р 59346	Частные и интегральные показатели рисков реализации угроз, направленных на нарушение функционирования системы в течение периода прогноза по ГОСТ Р 59346
Процесс определения архитектуры системы	См. ГОСТ Р 59347	То же, что для процесса приобретения продукции и/или услуг для системы
Процесс определения проекта	См. ГОСТ Р 59348	То же
Процесс системного анализа	См. ГОСТ Р 59349	То же
Процесс реализации системы	См. ГОСТ Р 59350	То же
Процесс комплексирования системы	См. ГОСТ Р 59351	То же
Процесс верификации системы	См. ГОСТ Р 59352	То же
Процесс передачи системы	См. ГОСТ Р 59353	То же
Процесс аттестации системы	См. ГОСТ Р 59354	То же
Процесс функционирования системы	См. ГОСТ Р 59355	То же
Процесс сопровождения системы	См. ГОСТ Р 59356	То же
Процесс изъятия и списания системы	См. ГОСТ Р 59357	То же

Далее для расчетов прогнозируемых рисков нарушения функциональной целостности системы излагается типовая модель, доведенная до реализации в национальных стандартах (см.. например, ГОСТ Р 59341, ГОСТ Р 59349).

4. Пример типовой модели для прогноза риска нарушения функциональной целостности системы

Предполагается изначальная функциональной целостность системы (в частном случае система – это «черный ящик»). В процессе функционирования в результате реализации возможных опасностей могут начать развиваться угрозы, приводящие к нарушению функциональной целостности системы. Начало (инициирование) каждого источника таких опасностей служит причиной последующих потенциальных нарушений. В системе осуществляется периодический контроль целостности.

Примечание. В приложении к каждой системе (и ее критичных элементов) понятие и показатели обеспечения и нарушения функциональной целостности должны быть конкретизированы на уровне правил, инструкций по эксплуатации, обязанностей должностных лиц и т.п.

В рамках модели развитие критичных ситуаций в системе считается не нарушающим функциональной целостности в течение заданного прогнозного периода времени, если к началу этого периода нарушение целостности отсутствует и в течение всего периода либо источники опасности не инициируются, либо после инициации происходит их оперативное выявление и принятие адекватных мер противодействия. Предполагается, что существуют не только средства диагностики (контроля) функциональной целостности, но и способы поддержания и/или ее восстановления при выявлении источников опасности или следов их инициации. Восстановление осуществляется лишь в период системного контроля.

За основу анализа принят следующий поэтапный алгоритм возникновения и реализации опасности: сначала источник опасности появляется и начинает инициироваться, а по прошествии свойственного ему пери-

ода инициации опасность разрастается до нарушения функциональной целостности системы. Если опасность постоянна (например, для опасного производства), выделяются приемлемый нормативный диапазон, который не должен нарушаться для показателей, характеризующих уровень опасности. Целостность считается нарушенной лишь после того, как инициировавшийся источник приводит к нарушению штатного режима функционирования (например, установленных пределов нормативного диапазона работы оборудования промышленного предприятия). Если инициировавшийся источник опасности был выявлен до наступления нештатной ситуации и приняты адекватные контрмеры, считается, что функциональная целостность системы не нарушена. Результатом применения очередной диагностики является полное восстановление нарушенной целостности системы до приемлемого уровня или подтверждение функциональной целостности при отсутствии ее нарушения – см. описание на рис. 4.

Модель позволяет оценить вероятность нарушения функциональной целостности системы в течение заданного периода времени. Именно эта вероятность с учетом последствий определяется как риск нарушения функциональной целостности в течение заданного периода прогноза с учетом предпринимаемых мер периодического контроля и восстановления, а также возможных последствий от нарушений. Достижение приемлемого уровня риска является следствием достаточно частого диагностирования и применения эффективных средств диагностики, контроля и восстановления целостности при существующих ограничениях.

Примечание. Существование средств гарантированного выявления источников опасности или следов их воздействия и существование способов поддержания нарушенной функциональной целостности системы являются необходимыми условиями применения модели.

Для описания процессов возникновения и выявления опасных воздействий на систему введены обозначения:

σ – частота возникновения источника опасности;

β – среднее время инициации с разрастанием опасности до нарушения целостности;

$T_{меж}$ – время между окончанием предыдущей и началом очередной диагностики;

$T_{диаг}$ – длительность диагностики, включая восстановление целостности;

$T_{зад}$ – длительность прогнозного периода времени.

Оценка риска нарушения целостности системы $R_{наруш.}$ в течение прогнозного периода $T_{зад}$ осуществляется по формуле:

$$R_{наруш.} = 1 - P_{возд.}, \quad (1)$$

где $P_{возд.}$ – это вероятность отсутствия нарушений целостности в течение $T_{зад.}$

Возможны два варианта:

— вариант 1 – заданный оцениваемый период $T_{зад}$ меньше периода между окончаниями соседних диагностик ($T_{зад} \geq T_{меж} + T_{диаг}$);

— вариант 2 — заданный оцениваемый период $T_{зад}$ больше или равен периоду между окончаниями соседних диагностик ($T_{зад} \geq T_{меж} + T_{диаг}$), т.е. за это время заведомо произойдет одна или более диагностик.

Для варианта 1 при условии независимости исходных характеристик вероятность $P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ отсутствия нарушений целостности в течение периода $T_{зад.}$ вычисляют по формуле (как распределение от суммы времен возникновения и инициации опасности на момент завершения периода прогноза $T_{зад}$ – см. рис. 1):

$$P_{возд\,(1)} = \begin{cases} \left(\sigma - \beta^{-1}\right)^{-1} \left\{\sigma e^{-T_{зад}/\beta} - \beta^{-1} e^{-\sigma T_{зад}}\right\}, если\ \sigma \neq \beta^{-1}, \\ e^{-\sigma T_{зад}} \left[1 + \sigma T_{зад}\right], если\ \sigma = \beta^{-1}. \end{cases} \quad (2)$$

Примечание — Эту же формулу используют для оценки вероятности отсутствия нарушений целостности без какой-либо диагностики.

Для варианта 2 при условии независимости исходных характеристик для расчетов возможны различные вероятностные меры.

Согласно первой мере вероятность $P_{возд(2)}$ отсутствия нарушений целостности в течение периода $T_{зад.}$ может быть вычислена по формуле:

$$P_{возд(2)} = P_{серед} + P_{кон}, \quad (3)$$

где $P_{серед}$ – вероятность отсутствия нарушений целостности в течение всех периодов между диагностиками, целиком вошедшими в $T_{зад}$. С учетом доли этих периодов $\frac{N(M_{меж}+T_{диаг})}{T_{диаг}}$ в общем оцениваемом периоде $T_{зад}$, расчет осуществляют по формуле

$$P_{серед} = \frac{N\left(T_{меж} + T_{диаг}\right)}{T_{зад}} \times \times P^{N}_{возд\,(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж} + T_{диаг}) \quad (4)$$

N – число периодов между диагностиками, которые целиком вошли в пределы времени Tзад, с округлением до целого числа, $N=[T_{зад}/(T_{меж} + T_{диаг})]$ — целая часть.;

$P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж}+T_{диаг})$ – вероятность отсутствия нарушений целостности за один период между диагностиками, целиком вошедший в пределы времени $T_{зад}$, вычисляют по формуле (2);

$P_{кон}$ – вероятность отсутствия нарушений целостности после последней диагностики (в конце $T_{зад}$). С учетом доли остатка $T_{ост}=T_{зад}- N(T_{меж}+T_{диаг})$ в общем прогнозном периоде $T_{зад}$ расчет осуществляют по формуле

$$P_{кон}=\frac{T_{ост}}{T_{зад}}\cdot P_{возд\,(1)}(\sigma,\beta,T_{меж},T_{диаг},T_{ост}); \quad (5)$$

Значение $P_{возд(1)}(s, b, T_{меж}, T_{диаг}, T_{ост})$ для остатка от задаваемого прогнозного периода вычисляют по формуле (2) с тем отличием, что вместо $T_{зад}$ стоит $T_{ост}$.

Другая возможная вероятностная мера для оценки вероятности $P_{возд(2)}$:

$$P_{возд\,(2)}=P_{серед}\cdot P_{кон}, \quad (6)$$

где

$$P_{серед}=P^{N}_{возд\,(1)}\left(\sigma,\beta,T_{меж},T_{диаг},T_{меж}+T_{диаг}\right), \quad (7)$$

$$P_{кон}=P_{возд\,(1)}\left(\sigma,\beta,T_{меж},T_{диаг},T_{ост}\right) \quad (8)$$

В отличие от меры (3) отклонения расчетной вероятности за счет более частого контроля и восстановления целостности практически трудноразличимы, что для аналитика скрывает эффективность этих мер противодействия в управлении рисками.

Примечание. Другие возможные показатели, модели и методы для оценки рисков описаны, например, в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 58494, ГОСТ Р 59339, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

5. Пример реализации

В России создан комплекс обеспечения техногенной безопасности на объектах газораспределения нефтегазовой отрасли, служащий ярким примером достижения прагматических эффектов с использованием предложенных методов аналитического прогнозирования рисков с учетом требований по защите информации. В созданном комплексе периферийные газорегуляторные пункты дополнительно оснащены датчиками вибрации (фиксирование землетрясения), пожара, наводнения, несанкционированного доступа, урагана, видеоизображение внутренней и внешней обстановки, а также интеллектуальными средствами реакции, способными реализовать процедуры распознавания, идентификации и раннего прогнозирования развития нештатных ситуаций. Реализованные технологические возможности использования космической связи позволяют реагировать за секунды. Эксплуатация комплекса в Калужской и Курской областях обеспечило безаварийное функционирование нефтегазовых объектов (до этого – по несколько аварийных ситуаций в год) и его применение обеспечило экономию 8,5 млрд рублей за 5 лет, что достигнуто за счет эффективного внедрения функций прогнозирования рисков и обеспечения техногенной безопасности в технологического процессы контроля и мониторинга газораспределения. Работа была удостоена премии Правительства РФ в области науки и техники [3].

Другие примеры извлечения прагматических эффектов с использованием прогнозирования рисков и учетом требований по защите информации приведены в ГОСТ Р ИСО 11231, ГОСТ Р 58494, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356 (к примеру, см. [19-22]).

Выводы

Предложенные модели и методы системного анализа защиты информации в стандартизованных процессах системной инженерии развивают сложившиеся подходы к прогнозированию рисков, обеспечению и повышению безопасности систем [23]. Использование предлагаемых моделей и методов до уровня рекомендуемых в национальных стандартах ГОСТ Р 59329 – ГОСТ Р 59357 позволяет предприятиям при сохранении их ответственности за обеспечение информационной безопасности перейти к прагматичному внедрению риск-ориентированного подхода. Это подразумевает появление и применение аналитических возможностей к решению обратных задач эффективного управления безопасностью, исходя из задаваемого уровня допустимого риска.

Появление возможностей системной инженерии в части прогнозирования рисков с учетом требований по защите информации позволяет подготовиться к вызовам ближайшего будущего, связанного с одной стороны с ростом неопределенностей и угроз, а с другой стороны – с резким усложнением различного рода систем, возрастанием объемов обрабатываемой ими информации.

DOI:10.21681/2311-3456-2022-6-71-82

Литература

1. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. /Под ред. Махутова Н.А./. М.: МГОФ «Знание», 1998-2022. Тома 1-64.
2. Костогрызов А.И. Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта / БИТ. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019, С. 220-229.
3. Костогрызов А.И., Степанов П.В., Нистратов А.А., Григорьев Л.И., Червяков Л.М. Прогнозирование рисков для обеспечения качества информации в сложных системах // Системы высокой доступности № 3, т.2, 2016, с. 25-37
4. Artemyev V., Kostogryzov A., Rudenko J., Kurpatov O., Nistratov G., Nistratov A. Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20-22, 2017, Milan, Italy, pp. 368-373
5. Kershenbaum V., Grigoriev L., Kanygin P. and Nistratov A. / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, pp. 55-79. DOI: 10.5772/intechopen.74963.
6. Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In “Safety and Reliability of Systems and Processes”, Gdynia Maritime University, 2020. pp. 153-174. DOI: 10.26408/srsp-2020
7. Kostogryzov A. Risks prediction for artificial intelligence systems using monitoring data. CEUR Workshop Proceedings. 2019. V. 2603. P. 29-33.
8. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364.
9. Kostogryzov A., Stepanov P., Nistratov A., Nistratov G., Atakishchev O. and Kiselev V. Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling. Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186-192.
10. Kostogryzov A.I. Analysis of the impact of information security on the performance of decision management process. CEUR Workshop Proceedings. 2021. V. 3035. P. 66-75.
11. Kostogryzov A.I., Avdonin R.Y., Nistratov A.A. The estimation of probabilistic risks for the performance of system human resource management process. CEUR Workshop Proceedings. 2021. V. 3035. P. 76-87.
12. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 287 p. DOI: 10.5772/intechopen.71396.
13. Васильев В.И., Кириллова А.Д., Вульфин А.М. Моделирование кибератак на объекты АСУ ТП с помощью нечетких когнитивных карт // Приоритетные направления развития науки и технологий: доклады XXVIII международной науч.- практич. конф.; под общ. ред. В.М. Панарина. — Тула: Инновационные технологии. 2021. — С. 132-132
14. Каляев И.А., Заборовский В.С., Антонов А.П. Архитектура реконфигурируемой гетерогенной распределенной суперкомпьютерной системы для решения задач интеллектуальной обработки данных в эпоху цифровой трансформации экономики // Вопросы кибербезопасности. 2019. № 5 (33). С. 2-11. DOI: 10.21681/231-3456-2019-3-02-11
15. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под. ред. Д.П. Зегжда. — М.: Горячая линия — Телеком, 2021. — 560 с
16. Костогрызов А.И., Нистратов А.А. Подходы к прогностической обработке данных в системах искусственного интеллекта. Часть 2. достижение практических эффектов. // ИТ-Стандарт. 2022. № 1 (30). С. 4-23.
17. Arpishkin M.I., Vulfin A.M., Vasilyev V.I., Nikonov A.V. Intelligent integrity monitoring system for technological process data. Journal of Physics: Conference Series. IOP Publishing. - 2019 — Vol. 1368, №. 5.- P. 1-16. DOI: 10.1088/1742-6596/1368/5/052029
18. Markov A., Markov G., Tsirlov V. Simulation of Software Security Tests by Soft Computational Methods. In Proceedings of the VIth International Workshop ‘Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security’ (IWCI 2019). (March 17-24, 2019 in Irkutsk, Baikalsk, Russia). Advances in Intelligent Systems Research vol. 169. Pp. 257-261. DOI: 10.2991/iwci-19.2019.45. DOI: 10.2991/iwci-19.2019.45.
19. Андрюхин Е.В., Ридли М.К., Правиков Д.И. Прогнозирование сбоев и отказов в распределенных системах управления на основе моделей прогнозирования временных рядов // Вопросы кибербезопасности. 2019. № 3 (31). С. 24-32. DOI: 10.21681/2313456-2019-3-24-32
20. Костогрызов А.И. Анализ направлений развития международной стандартизации в области системной и программной // Костогрызов А.И. ИТ-Стандарт. 2015. № 3 (4). С. 37-48.
21. Марков А.С., Тимофеев Ю.А. Стандарты кибербезопасности Четвертой промышленной революции и Индустрии 4.0 // Защита информации. Инсайд. 2021. № 3 (99). С. 54-60.
22. Петренко С.А., Петренко А.С. Практика применения ГОСТ Р МЭК 61508 // Защита информации. Инсайд. 2016. № 2 (68). С. 42-49.
23. Костогрызов А.И. Вероятностное моделирование в системной инженерии. В сборнике: Россия в XXI веке в условиях глобальных вызовов: проблемы управления рисками и обеспечения безопасности социально-экономических и социально-политических систем и природно-техногенных комплексов. Сборник материалов Всероссийской научно-практической конференции. Российская академия наук, Международный независимый эколого-политологический университет, Государственный университет управления. Москва, 2022. С. 214-219.

ON MODELS AND METHODS OF PROBABILISTIC ANALYSIS OF INFORMATION SECURITY IN STANDARDIZED PROCESSES OF SYSTEM ENGINEERING

***Kostogryzov A.I.*[2]**

Purpose: *rational and description of the methodological apparatus of system engineering in terms of risk prediction, taking into account the requirements for information protection*

Research methods include: *methods of probability theory, risk-oriented models for predictive analysis of standardized processes of system engineering.*

Result: *interrelated models and methods systematized for use in the planning and implementation of standardized processes of system engineering are described. Their use makes it possible to analyze the impact of information security in terms of predicted risks. Methods and models are implemented in a set of system engineering standards and analytically support the effective implementation of agreement, organizational project-enabling, technical management and technical processes according to GOST R 57193 (ISO/IEC/IEEE 15288) in relation to systems for various purposes (a total of 30 processes). The proposed models and methods of system analysis of information security in standardized processes of system engineering develop established approaches to risk prediction, ensuring and improving system security. The use of the proposed models and methods in the life cycle of systems helps to identify «bottlenecks», rational ways to reduce risks in the implemented standardized processes, taking into account the requirements for information protection, supports the making decisions in analytical problems of system engineering.*

Scientific novelty: *the proposed methodological apparatus develops the existing approaches to risk prediction, ensuring and improving systems security. The ideas are implemented in the national standards GOST R 59329 – GOST R 59357. They allow enterprises to move to the pragmatic implementation of a risk-based approach using the analytical capabilities of solving inverse problems of effective security control, based on the specified level of acceptable risk.*

Keywords: *risk-based approach, probabilistic models, information security, risk prediction, systems engineering standards, systems analysis*

References

1. Bezopasnost' Rossii. Pravovye, social'no-jekonomicheskie i nauchno-tehnicheskie aspekty. /Pod red. Mahutova N.A./. M.: MGOF «Znanie», 1998-2022. Toma 1-64.
2. Kostogryzov A.I. Prognozirovanie riskov po dannym monitoringa dlja sistem iskusstvennogo intellekta / BIT. Sbornik trudov Desjatoj mezhdunarodnoj nauchno-tehnicheskoj konferencii – M.: MGTU im. N.Je. Baumana, 2019, C. 220-229.
3. Kostogryzov A.I., Stepanov P.V., Nistratov A.A., Grigor'ev L.I., Chervjakov L.M. Prognozirovanie riskov dlja obespechenija kachestva informacii v clozhnyh sistemah // Sistemy vysokoj dostupnosti No3, t.2, 2016, s. 25-37
4. Artemyev V., Kostogryzov A., Rudenko J., Kurpatov O., Nistratov G., Nistratov A. Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20-22, 2017, Milan, Italy, pp. 368-373
5. Kershenbaum V., Grigoriev L., Kanygin P. and Nistratov A. / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, pp. 55-79. DOI: 10.5772/intechopen.74963.
6. Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In "Safety and Reliability of Systems and Processes", Gdynia Maritime University, 2020. pp. 153-174. DOI: 10.26408/srsp-2020
7. Kostogryzov A. Risks prediction for artificial intelligence systems using monitoring data. CEUR Workshop Proceedings. 2019. V. 2603. P. 29-33.
8. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364.
9. Kostogryzov A., Stepanov P., Nistratov A., Nistratov G., Atakishchev O. and Kiselev V. Risks Prediction and Processes Optimization for

2 Andrey I. Kostogryzov, Dr.Sc., Professor, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia. E-mail: Akostogr@gmail.com

Complex Systems on the Base of Probabilistic Modeling. Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186-192.
10. Kostogryzov A.I. Analysis of the impact of information security on the performance of decision management process. CEUR Workshop Proceedings. 2021. V. 3035. P. 66-75.
11. Kostogryzov A.I., Avdonin R.Y., Nistratov A.A. The estimation of probabilistic risks for the performance of system human resource management process. CEUR Workshop Proceedings. 2021. V. 3035. P. 76-87.
12. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 287 p. DOI: 10.5772/intechopen.71396.
13. Vasil'ev V.I., Kirillova A.D., Vul'fin A.M. Modelirovanie kiberatak na ob#ekty ASU TP s pomoshh'ju nechetkih kognitivnyh kart // Prioritetnye napravlenija razvitija nauki i tehnologij: doklady XXVIII mezhdunarodnoj nauch.- praktich. konf.; pod obshh. red. V.M. Panarina. — Tula: Innovacionnye tehnologii. 2021. — S. 132-132
14. Kaljaev I.A., Zaborovskij V.S., Antonov A.P. Arhitektura rekonfiguriruemoj geterogennoj raspredelennoj superkomp'juternoj sistemy dlja reshenija zadach intellektual'noj obrabotki dannyh v jepohu cifrovoj transformacii jekonomiki // Voprosy kiberbezopasnosti. 2019. No 5 (33). S. 2-11. DOI: 10.21681/231-3456-2019-3-02-11
15. Kiberbezopasnost' cifrovoj industrii. Teorija i praktika funkcional'noj ustojchivosti k kiberatakam / Pod. red. D.P.Zegzhda. — M.: Gorjachaja linija — Telekom, 2021. — 560 s
16. Kostogryzov A.I., Nistratov A.A. Podhody k prognosticheskoj obrabotke dannyh v sistemah iskusstvennogo intellekta. Chast' 2. dostizhenie prakticheskih jeffektov. // IT-Standart. 2022. No 1 (30). S. 4-23.
17. M.I. Arpishkin, A.M. Vulfin, V.I. Vasilyev, A.V. Nikonov. Intelligent integrity monitoring system for technological process data. Journal of Physics: Conference Series. IOP Publishing. - 2019 — Vol. 1368, No. 5.- P. 1-16. DOI: 10.1088/1742-6596/1368/5/052029
18. Markov A., Markov G., Tsirlov V. Simulation of Software Security Tests by Soft Computational Methods. In Proceedings of the VIth International Workshop 'Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security' (IWCI 2019). (March 17-24, 2019 in Irkutsk, Baikalsk, Russia). Advances in Intelligent Systems Research vol. 169. Pp. 257-261. DOI: 10.2991/iwci-19.2019.45. DOI: 10.2991/iwci-19.2019.45.
19. Andrjuhin E.V., Ridli M.K., Pravikov D.I. Prognozirovanie sboev i otkazov v raspredelennyh sistemah upravlenija na osnove modelej prognozirovanija vremennyh rjadov // Voprosy kiberbezopasnosti. 2019. No 3 (31). S. 24-32. DOI: 10.21681/231-3456-2019-3-24-32
20. Kostogryzov A.I. Analiz napravlenij razvitija mezhdunarodnoj standartizacii v oblasti sistemnoj i programmnoj // Kostogryzov A.I. IT-Standart. 2015. No 3 (4). S. 37-48.
21. Markov A.S., Timofeev Ju.A. Standarty kiberbezopasnosti Chetvertoj promyshlennoj revoljucii i Industrii 4.0 // Zashhita informacii. Insajd. 2021. No 3 (99). S. 54-60.
22. Petrenko S.A., Petrenko A.S. Praktika primenenija GOST R MJeK 61508 // Zashhita informacii. Insajd. 2016. No 2 (68). S. 42-49.
23. Kostogryzov A.I. Verojatnostnoe modelirovanie v sistemnoj inzhenerii. V sbornike: Rossija v HHI veke v uslovijah global'nyh vyzovov: problemy upravlenija riskami i obespechenija bezopasnosti social'no-jekonomicheskih i social'no-politicheskih sistem i prirodno-tehnogennyh kompleksov. Sbornik materialov Vserossijskoj nauchno-prakticheskoj konferencii. Rossijskaja akademija nauk, Mezhdunarodnyj nezavisimyj jekologo-politologicheskij universitet, Gosudartvennyj universitet upravlenija. Moskva, 2022. S. 214-219.