УДК 338.3:621.391:[004.5+004.67]
Оригинальная статья
https://doi.org/10.21683/1729-2646-2024-24-4-58-64

О некоторых случаях количественной оценки ущерба технической системе

On some cases of quantitative estimation of damage to a technological system

Лобач Д.И.
Lobach D.J.
Департамент по ядерной и радиационной безопасности Министерства по чрезвычайным ситуациям Республики Беларусь, Беларусь, Минск
Department of Nuclear and Radiation Safety, Ministry of Emergency Situations of the Republic of Belarus, Belarus, Minsk
lobachd@yandex.ru

Лобач Д.И.

Резюме. Цель. *Цель исследований – сформулировать и продемонстрировать дополнительные экспертные возможности для рассмотрения проекта технических систем в контексте оценки нанесения ему возможного ущерба, которые могут быть использованы для относительного сравнения проектируемых, планируемых или применяемых объектов анализа, выработки стратегий и рекомендаций для дальнейшей эксплуатации.* **Метод.** *В статье применяются методы относительного анализа количественных закономерностей.* **Результат.** *Использование дополнительных экспертных подходов позволит провести наработку опыта для сравнения проектов, определение потенциальных их возможностей в разрезе осуществления дальнейших модификаций и модернизаций.* **Вывод.** *Предложенный подход относительного анализа количественных закономерностей позволяет выработать стратегии и рекомендации для выбора среди конкурирующих технологических решений, принятия решения по управлению системой, планировать финансирование производств на основании имеющихся, установленных экспертами, недостатков безопасности и «слабых звеньев» в техническом обеспечении или управлении организацией.*

Abstract. Aim. *The research aims to define and demonstrate additional expert-based methods of examining technological systems in the context of possible damage assessment, that can be used for relative comparison of designed, planned or operated objects of analysis, development of strategies and recommendations for further operation.* **Method.** *The paper uses methods of relative analysis of quantitative patterns.* **Result.** *The use of additional expert-based methods will allow building know-how to compare technological system designs in the absence of operational experience, to identify their potential capabilities in the context of further modifications and upgrades.* **Conclusion.** *The proposed method of relative analysis of quantitative patterns allows developing strategies and recommendations for choosing among competing technological solutions, system management decision-making, and planning production funding based on existing, expert-defined safety and security deficiencies and "weak links" in the technological capabilities or management of a company.*

Ключевые слова: *экспертная оценка, безопасность, эксплуатационный опыт, сэйфеометрика, несанкционированные действия, ущерб, техническая система*
Keywords: *expert assessment, safety, operational experience, safeometrics, unauthorized actions, damage, technical system*

Для цитирования: *Лобач Д.И. О некоторых случаях количественной оценки ущерба технической системе // Надежность. 2024. №4. С. 58-64. https://doi.org/10.21683/1729-2646-2024-24-4-58-64*
For citation: *Lobach D.J. On some cases of quantitative estimation of damage to a technological system. Dependability 2024;4:58-64. https://doi.org/10.21683/1729-2646-2024-24-4-58-64*

Поступила: *22.06.2024* / **После доработки:** *21.08.2024* / **К печати:** *18.11.2024*
Received on: *22.06.2024* / **Revised on:** *21.08.2024* / **For printing:** *18.11.2024*

Введение

Для успешного продвижения коммерческих проектов устройств, систем и технологий в промышленности, атомной энергетике производителю важно продемонстрировать преимущества новых решений в технике [1-3]. При выборе между несколькими дорогостоящими проектами заказчику тоже следует проводить свои собственные оценки технологий, обращаться к экспертам для осуществления независимого анализа проектов, которые еще не имеют достаточного количества экспериментальных и эксплуатационных данных. Зачастую действия заказчика мотивируются также тем, чтобы получить от реализации проекта значимый экономический эффект в недолгосрочной перспективе. Однако при этом иногда под сомнение могут попадать как выбор неапробированных технологий безопасности, так состав и качество применяемых инновационных технических систем (далее – ТС) и оборудования, а сам проект может потом дорабатываться при своей реализации с использованием технических решений в ходе модификаций. По этой причине не существует абсолютно одинаковых референтных проектов.

Недостаточное количество опытных данных является основной проблемой проведения традиционных экспертных оценок и экспертиз, упомянутых в литературе как процедуры «*safety assessment*», «*risk assessment*», «*security assessment*», на которых базируются подходы, рассматриваемые, например, в документах Международного агентства по атомной энергии (МАГАТЭ) в контексте детерминистического и вероятностного анализа.

ТС являются структурно-сложными, и для анализа их безопасности разработаны некоторые комплексные подходы, например, в разрезе вопросов качественной оценки состояния безопасности и синтеза рисков в управлении безопасностью [4, 5]. В работах [6, 7] отмечались направления развития вычислительного аппарата для проведения экспертных оценок проектов в разрезе вспомогательной концепции, основанной на аналогиях с подходами *хемометрики*.

Следует отметить, что оценка проекта может быть проведена как в части параметров его функционирования, так и для характеристик препятствующих, сдерживающих работу. К числу последних можно отнести внутренние и внешние факторы, угрозы, такие как *несанкционированные (злоумышленные) действия* в отношении проекта, например, случайные непреднамеренные действия непрофессионала из-за низкой культуры безопасности, намеренные акции инсайдера (внутреннего нарушителя), внешняя диверсия, саботаж [8–10].

Проведение оценки ущерба проекту позволит определить значимость и критическую величину факторов, угнетающих производство. В дальнейшем, каждому уровню ущерба будут соответствовать те или иные последствия, к которым следует либо подготовиться, либо их предотвратить. Рекомендации экспертов по таким вопросам могут являться существенными для создания информационного фона и условий реализации новых проектов или определения их конкурентоспособности на рынке технологий.

В силу специфических потребностей и развития личности в цифровую эпоху у людей практически сформировалось клиповое мышление [11]. Эксперты и специалисты управления предпочитают получать короткую и наглядную информацию, прослеживается их ориентация на быстрый результат. Влияние человеческого фактора в человеко-машинных ТС присутствует постоянно, и поэтому для опасных производств проводится всестороннее интенсивное изучение этого явления [12–16]. В такой ситуации подходящими для оценок будут простые закономерности между параметрами проекта, которые позволяют проанализировать и получить ответ, принять решение за непродолжительное время.

При недостатке эксплуатационных данных и опыта для технических проектов вспомогательные методы *сэйфеометрики* для оценки параметров технологий позволяют развивать дополнительные экспертные возможности [7].

1. Основные направления экспертного рассмотрения проекта в контексте оценки нанесения ему возможного ущерба

Главная задача аналитиков при проведении экспертных оценок – понять и интерпретировать текущее состояние производственной системы в разрезе оценки дальнейших затрат при использовании заявленных в проекте технологий, определить уровень безопасности в ТС и ее компонентах в контексте недостижения или близости *наихудшего события* (далее – НС) в ТС, т.е. когда будет причинен наибольший урон технике, а экономические затраты на восстановление значительны или превосходят уже выделенные (запланированные). Эксперт определяет, насколько далеко в технологическом смысле (с учетом износа, порчи, устаревания техники) от текущего состояния находится НС, при правильной и полной эксплуатации оборудования проекта, деградации и старении оборудования, злоумышленных действиях и т.п.

Эксперт должен также оценить влияние на состояние ТС самой эксплуатации, использования технологий, влияние внутренних и внешних факторов на состояние и функционирование глубокоэшелонированной защиты *систем безопасности* (далее – СБ), способности производственной системы для поддержания условий безопасной эксплуатации.

Обычно эксперт может ограничиться рассмотрением соответствия технологии требованиям нормативной и проектной документации, где имеются конкретные

положения, которые редко охватывают комплексные ситуации. Этому также способствуют специализации экспертов и ограниченность в их компетентности. Например, в атомной промышленности разделяются анализ и рассмотрение ядерной и радиационной безопасности (аспекты функционирования ядерных технологий) и ядерной физической безопасности (вопросы физической защиты и сохранности ядерного и радиоактивного материала). Хотя МАГАТЭ продвигает концепцию понимания синергии этих вопросов, но на уровне рассмотрения вопросов специалистами и экспертами доминирует узкая специализация.

Для более детального, полного и всестороннего рассмотрения, анализа и оценок проекта надо уделить внимание комплексным вопросам, таким как:

– построение системной деятельности по обеспечению безопасности производства (должны быть понятная организационная структура, реальная компетентность руководителей, ясная система контроля исполнения и т.п.);

– поиск «слабых звеньев» в СБ и организационной структуре (уменьшение влияния человеческого фактора, дублирование и контроль управляющих систем, приоритетное их диагностирование и техническое обслуживание);

– планирование адекватного ответа угрозам, в т.ч. в контексте проектной угрозы (рациональность построения систем проекта и их компонентов, проведение организационных мероприятий по компенсации «слабых звеньев» и недостатков и т.п.);

– планирование экономических затрат на обеспечение безопасности производства (заблаговременное выделение финансовых средств и пополнение ресурсов, поддержание требуемых запасов материальных ценностей).

По результатам экспертного анализа заказчику проекта или оценки важно представлять достоинства и недостатки технологии с целью устойчивой ее эксплуатации, планирования своего бюджета [3]. Такой анализ можно проводить путем сравнения с референтными образцами, ранее реализованными аналогами, технологиями конкурентов или в рамках дихотомии «безопасно» / «небезопасно» (рискованно).

2. Методология

В работе [6] говорилось, что подходящие априорные параметры проекта могут быть использованы для сравнения характеристик планируемых к созданию технологий с уже существующими, реализованными конструкциями для которых имеется достаточное количество эксплуатационных данных, апробированный эксплуатационный опыт.

В концепции сэйфеометрики [7] можно устанавливать связи и зависимости между параметрами как для поиска преимуществ новых проектов, так и для определения их недостатков и «слабых звеньев». Анализ и рекомендации экспертов в этом направлении будут влиять на уточнение для проекта соотношения «польза» / «вред», определения приемлемости новой технологии для общества.

Применяемые экспертом дополнительные методы анализа должны рассматривать проект вглубь с целью поиска полезных решений и неудачных суперпозиций элементов в ТС. В наилучшем случае такие методы должны быть подобны и инвариантны при переходе рассмотрения от общего к частному и обратно, описаны в регламентированных рекомендациях, но следует допустить и применение экспертом своих «*know-how*».

Говоря об использовании для экспертных оценок величины степени опасности α [6], следует сказать, что этот подход может быть применим как для ТС в целом, так и для конкретных промышленных систем, узлов, устройств и элементов. В обоих случаях степень опасности определяется как $\alpha=N_{СБ}/M_{ф}$, где $N_{СБ}$ – количество СБ для рассматриваемого технического объекта, $M_{ф}$ – количество проектных или запроектных факторов опасности (предписанных событий или отказов или иного, на усмотрение эксперта) для этого технического объекта.

Как было отмечено в [6], при $\alpha\leq1$ применение СБ является более эффективным. В других случаях, когда $\alpha>1$, следует учесть во внимание природу факторов опасности, их суперпозицию (в разрезе усиления, умножения и синергии), действительно ли им необходимо противопоставить несколько СБ. В этом смысле следует отдавать предпочтение не активным СБ, а пассивным, следящим системам СБ. В большинстве технических случаев активные СБ требуют использования резервных источников энергии, а также дополнительных систем управления и энергонезависимой автоматизации. Такие технологические элементы могут иметь «слабые звенья», а при проверке их функционирования в ходе производственных экспериментов не всегда удается создать или смоделировать фактические условия их срабатывания.

На практике для α можно получить проектное и фактическое значения. Важно рассмотреть задействованное количество СБ и фактическое количество факторов опасности. Их соотношение может оказывать влияние на экономический вклад в стоимость проекта. В этом контексте можно проанализировать, был ли осуществлен запас свойств для безопасности или тут проведена необоснованная экономия средств при реализации проекта ТС.

Особое значение увеличению количества СБ и их разнообразию придается в проекте при борьбе с несанкционированными действиями. Это связано с противодействием ущербу технологии от них и минимизации его последствий.

При нанесении ущерба ТС или элементу уровень их безопасности не остается неизменным, он понижается. Сам ущерб априори предполагает нанесение определенного урона проекту. Основной единицей измерения ущерба будет денежная единица стоимости нанесенного

урона (технике, организационной структуре, ресурсам организации и т.п.).

Тем не менее, если считать, что ущерб был нанесен (состоялся), то уровень безопасности тоже был изменен или систематически понижен. Будем полагать, что любой ущерб можно связать с эквивалентом безопасности, а суммарный ущерб – с эквивалентом для суммарной безопасности и т.д.

Явлению ущерба от случайных непреднамеренных действий персонала можно сопоставить статистический разброс Δ для значения уровня безопасности $\bar{Q}$, связанного с определенным уровнем культуры безопасности в организации: $\bar{Q} \pm \Delta$.

В ходе спланированного несанкционированного действия величина существующего уровня безопасности $\bar{Q}$ будет уменьшена систематическим образом. При диверсии конечный уровень безопасности $Q_Д$ будет меньше $\bar{Q}$ на величину эквивалента ущерба W_Σ от вреда диверсии D: $Q_Д = \bar{Q} - W_\Sigma$.

Диверсии и саботаж обычно проводятся в отношении рабочих систем производства. Предприятия являются привлекательными для проведения несанкционированных действий с точки зрения своего уровня технологической насыщенности. Техника будет более уязвимой, чем людские, рабочие или управленческие ресурсы в организации. Поврежденные элементы технологий зачастую нельзя быстро исправить, технические мероприятия замены, ремонта и диагностики являются длительными, требуются дополнительные незапланированные экономические средства и ресурсы, проведение возможных необходимых заказов комплектующих на других производствах и др.

Под технологической насыщенностью проекта (в контексте оснащенности рабочим оборудованием, техническими комплексами и т.п.) будем понимать величину $\Theta=1/\tau=N_{РС}/N_{СБ}$, где τ – уровень технической оснащенности СБ [6], $N_{РС}$ – количество рабочих систем (далее – РС), $N_{СБ}$ – количество СБ.

При $\Theta<1$ на одну РС приходится несколько СБ и поэтому имеется запас безопасности. Если $\Theta>1$, то имеется потенциальный дефицит безопасности (одна СБ приходится на несколько РС). Когда на одну РС приходится одна СБ ($\Theta=1$), то такая ситуация может быть присуща простым устройствам (например, механизму включения соответствует механизм выключения и всего в ТС имеется два состояния [7]).

Полагаем, что ущерб производству наносится через вывод из строя РС и (или) СБ, которые все функционируют независимо друг от друга. РС сгруппированы от простых к сложным. Сложная ТС может быть рассмотрена как совокупность простых. Комплексы технологии и производства отличаются друг от друга только количеством этих ТС и их соотношением.

Вред, который наносит злоумышленник, связан с выводом из строя СБ, которые отвечают за функционирование тех или иных РС (стратегия нанесения умышленного ущерба). Вывод из строя СБ будет соответствовать выводу из строя и РС. Если РС была выведена из строя, то можно полагать, что ответственная за нее СБ не сработала качественно. Величина ущерба от вывода из строя каждой СБ пропорциональна риску ущерба. Предположим, что действия злоумышленника (вред) D связаны с выводом из строя СБ ($D \propto N_{СБ}$), которые по своим свойствам тождественны и независимы. Из теории вероятностей для независимых событий величина суммарного ущерба W_Σ будет кратна произведению рисков ущерба при выводе из строя каждой СБ, которая подверглась несанкционированному действию. Такая ситуация подходит для случая с $\Theta=1$. Однако на практике следует более детально учитывать соотношение $N_{РС}$ и $N_{СБ}$.

Если $\Theta<1$, то при запасе безопасности СБ могут быть связаны друг с другом, задублированы. Такая система будет безопасной. Уровень ее безопасности не будет быстро понижаться. При этом величина суммарного ущерба стремиться к предельному ущербу $W_\Sigma \to W_{КР}$. Эта величина связана с достижением системой минимального уровня безопасности от диверсии или саботажа, с экономической эффективностью проекта в этом случае.

При $\Theta>1$ системе возможно нанесение серьезных повреждений. Последовательный выход нескольких СБ из строя определяет значительное увеличение ущерба и понижение уровня безопасности. Системе может быть нанесен критический вред $D_{КР}$ (соответствует выходу из строя критического количества СБ), и тогда ее функционирование будет экономически неэффективно. Для такого значения Θ можно полагать, что мы будем иметь дело с рискованной системой.

На основании определения Θ для указанных случаев соотношения $N_{РС}$ и $N_{СБ}$ изменение W_Σ при нанесении вреда злоумышленником D может быть описано эмпирическим способом с использованием степенных зависимостей типа $W_\Sigma = D^\Theta$ и представлено на рис. 1.

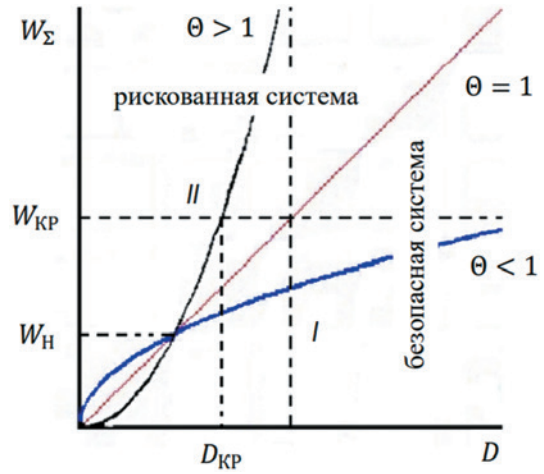

Рис. 1. Зависимость величины суммарного ущерба W_Σ для разных случаев технологической насыщенности проекта Θ

Системы с $\Theta<1$ в области I (см. рис. 1) можно отнести к безопасным системам, для которых риск серьезных по-

вреждений (ущерба) низкий. Предположим, что целью несанкционированного действия является нанесение вреда D_{KP}. Тогда изменение уровня безопасности Q ограничивается критическим изменением уровня безопасности, соответствующим W_{KP}, которое характеризует и формирует понимание устойчивости экономической эффективности проекта при несанкционированных действиях. Безопасные системы функционируют в диапазоне $W_\Sigma<W_{KP}$, но при $D>D_{KP}$.

При $\Theta>1$ в области *II* (см. рис. 1) для ТС характерен высокий риск серьезных повреждений (нанесения существенного ущерба от причинения вреда). Рискованные системы не будут функционировать при $D>D_{KP}$, поскольку $W_\Sigma>W_{KP}$, т.е. наступит состояние, когда цель несанкционированного действия будет достигнута.

Если $W_\Sigma \le W_H$, то можно полагать, что ТС находится в состоянии, когда величина причиненного ей ущерба не превышает тех масштабов, которые обусловлены существующим уровнем культуры безопасности в организации, т.е. $W_H=\Delta$.

Проведем анализ изменения величины суммарного ущерба W_Σ для ТС при разных степенях опасности α.

При неизменной величине количества проектных и (или) запроектных факторов опасности для технического объекта, увеличение нанесенного вреда (при выводе из строя СБ) приводит к повышению суммарного ущерба, поэтому решением уравнения $dW_\Sigma = \alpha \times D \times d\mathrm{D}$ будет функция типа $W_\Sigma = \alpha \times \frac{D^2}{2} + d$, где d – коэффициент. На рис. 2 представлены функции указанного вида для нескольких значений степеней опасности α ($\alpha_1<\alpha_2<\alpha_3$, d=0).

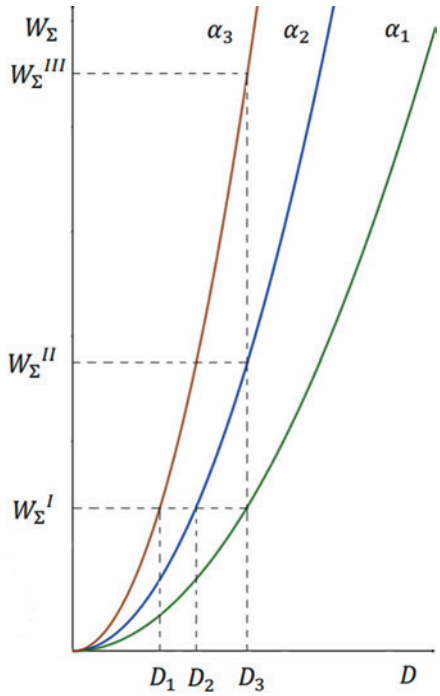

Рис. 2. Зависимость величины суммарного ущерба W_Σ для разных случаев степеней опасности α

ТС с α_1 является более интеллектуальной, поскольку ее управление использует меньшее количество систем или элементов безопасности для нейтрализации факторов опасности, чем для α_3 (более простая ТС). Следует отметить, что одинаковый вред нанесет меньший ущерб в интеллектуальной системе, чем в простой ($D=\mathrm{const}, W_\Sigma^{I} < W_\Sigma^{II} < W_\Sigma^{III}$). Для нанесения одинакового ущерба в отношении интеллектуальной системы необходимо совершить более тяжкое несанкционированное действие, чем в отношении простой ($W_\Sigma=\mathrm{const}, D_1 < D_2 < D_3$).

Из анализа функций (см. рис. 2) видно, что простая система быстрее уменьшает безопасность, чем интеллектуальная [7]. Одинаковый вред нанесет простой системе бóльший ущерб, чем интеллектуальной, где имеется запас безопасности. Для одинакового ущерба простой системе надо нанести меньше вреда.

С использованием дополнительных аналитических инструментов эксперт в ходе проведения своей работы, на основании полученных данных может предлагать изменения в технические проекты в части повышения их уровня безопасности, технологической насыщенности проекта, изменения состава оборудования систем управления и его качества, внесения изменений в системы «человек-человек» и «человек-машина» с целью уменьшения их уязвимости к несанкционированным действиям.

3. О выводах эксперта, выработке им стратегий и рекомендаций

По результатам проведенного анализа квалифицированный эксперт должен как описать и представить уровень текущего состояния безопасности производства, так и предложить стратегии и рекомендации по повышению уровня безопасности или его поддержании на уровне приемлемых потерь и ущербов. Глубина оценки зависит от компетентности эксперта и полноты доступа к информации о проекте, об имеющемся эксплуатационном опыте, характеристиках аналогов, референтных и конкурирующих технологиях.

Чтобы нанесенный ТС вред был незначительным, она должна быть интеллектуальной [7], иметь противовесы, дублирование СБ, высокий уровень контроля, самозащищенности, обладать свойством самовосстановления, быть устойчивой к несанкционированным воздействиям. Такие свойства проекта недостаточно указать в общем виде в нормативных документах. Поскольку они являются комплексными, то на практике их трудно проверить и проконтролировать. На производстве должна быть разработана система мер по постановке под контроль мероприятий самовосстановления и самозащищенности (во всех аспектах, рекомендованных экспертом), контроля «слабых звеньев».

Следует отметить, что некомпетентно проведенный анализ способствует множественности последующих

специализированных оценок, которые будут нужны заказчику. Такая ситуация обычно затрудняет выработку в организации системных мер по управлению производством.

Качественно проведенная оценка аспектов функционирования проекта и его безопасности на основании текущих и (или) проектных характеристик должна также включать:

– полезные эксплуатационные стратегии (режимы эксплуатации, проведение модификаций, модернизаций и т.п.);

– стратегии безопасности (для повышения или поддержания достигнутого уровня безопасности);

– стратегии локализации недостатков проекта (с обоснованием причин);

– стратегии минимизации возможного ущерба (при определении «слабых звеньев», недостатков проекта, влиянии человеческого фактора и т.п.);

– экономические стратегии развития и устойчивости производства (в технологическом смысле, с акцентом на восстановление и защищенность).

Использование дополнительных экспертных подходов [4–7] позволит провести наработку опыта для сравнения проектов, определения потенциальных возможностей в разрезе осуществления дальнейших модификаций и модернизаций.

Выводы

Применению прогнозных дополнительных методов оценки технологий следует уделять внимание как на этапе выбора конкурирующих технологических решений, так и в дальнейшем, при принятии решений в ходе управления. Если же проект уже принят к реализации, то независимые экспертные оценки могут быть использованы для планирования финансирования производственного процесса на основании имеющихся, установленных экспертами недостатков безопасности и «слабых звеньев» в техническом обеспечении или управлении организацией.

Библиографический список

1. Safety assessment for facilities and activities. General safety requirements. International Atomic Energy Agency. IAEA safety standards series, no. GSR Part 4 (Rev. 1), IAEA, Vienna, 2016.

2. Safety of nuclear power plants: design. Specific safety requirements. International Atomic Energy Agency. IAEA safety standards series, no. SSR-2/1 (Rev. 1), IAEA, Vienna, 2016.

3. SPESS F Document Preparation Profile (DPP) Version 4 dated 06 October 2022. DS537. Safety demonstration of innovative technology in power reactor designs [Электронный ресурс] // INTERNATIONAL ATOMIC ENERGY AGENCY. 2022. URL:https://www.iaea.org/sites/default/files/dpp537.pdf (дата обращения: 21.06.2024).

4. Бочков А.В. О методах качественной оценки состояния безопасности структурно-сложных систем // Надежность. 2020. № 20(3). С. 34-46. DOI: 10.21683/1729-2646-2020-20-3-34-46

5. Бочков А.В. О методе синтеза рисков в управлении безопасностью структурно-сложных систем // Надежность. 2020. № 20(1). С. 57-67. https://doi.org/10.21683/1729-2646-2020-20-1-57-67

6. Лобач Д.И. О развитии экспертных возможностей для рассмотрения проектов оборудования и технологических решений // Системный анализ и прикладная информатика. 2023. № 2. С. 38-41. DOI: 10.21122/2309-4923-2023-2-38-41

7. Лобач Д.И. Новые проблемы, методология и возможности сэйфеометрики // Промышленная безопасность. 2023. № 01. С. 34-36.

8. Nuclear security culture. Series IAEA nuclear security series, No. 7, IAEA, Vienna, 2008.

9. Preventive and protective measures against insider threats. Series IAEA nuclear security series, No. 8-G (rev. 1), IAEA, Vienna, 2020.

10. National nuclear security threat assessment, design basis threats and representative threat statements. Series IAEA nuclear security series, No. 10-G (Rev. 1), IAEA, Vienna, 2021.

11. Ковалев М.М. Образование для цифровой экономики // Цифровая трансформация. 2018. № 1(2). С. 37–42.

12. Человеческий фактор и безопасность ядерных установок. Материалы Международной конференции МК-2000. Москва, Обнинск: ОНИЦ «Прогноз», 2001.

13. Абрамова В.Н. Организационная психология, организационная культура и культура безопасности в атомной энергетике. Москва, Обнинск: ИГ – СОЦИН, 2009.

14. Safety culture, Safety series, No.75-INSAG-4, a report by the International Nuclear Safety Advisory Group, IAEA, Vienna, 1991.

15. Examples of safety culture practices, Safety reports series, No.1, IAEA, Vienna, 1997.

16. Key practical issues in strengthening safety culture, Safety series, No.INSAG-15, a report by the International Nuclear Safety Advisory Group, IAEA, Vienna, 2002.

References

1. Safety assessment for facilities and activities. General safety requirements. International Atomic Energy Agency. IAEA safety standards series, no. GSR Part 4 (Rev. 1). Vienna; 2016.

2. Safety of nuclear power plants: design. Specific safety requirements. International Atomic Energy Agency. IAEA safety standards series, no. SSR-2/1 (Rev. 1). Vienna; 2016.

3. SPESS F Document Preparation Profile (DPP) Version 4 dated 06 October 2022. DS537. Safety demonstration of innovative technology in power reactor designs.

International Atomic Energy Agency; 2022. (accessed 21.06.2024). Available at: https://www.iaea.org/sites/default/files/dpp537.pdf.

4. Bochkov A.V. On the methods of qualitative estimation of the safety state of structurally complex systems. *Dependability* 2020;20(3):34-46. DOI: 10.21683/1729-2646-2020-20-3-34-46.

5. Bochkov A.V. On the method of risk synthesis in the safety management of structurally complex systems. *Dependability* 2020;20(1):57-67. https://doi.org/10.21683/1729-2646-2020-20-1-57-67.

6. Lobach D.J. About development of expert possibilities for consideration of equipment projects and technological decisions. *System analysis and applied information science* 2023;(2):38-41. DOI: 10.21122/2309-4923-2023-2-38-41. (in Russ.)

7. Lobach D.J. [New problems, methodology, and capabilities of safeometrics]. *Promyshlennaya bezopasnost* 2023;1:34-36. (in Russ.)

8. Nuclear security culture. Series IAEA nuclear security series, No. 7. Vienna; 2008.

9. Preventive and protective measures against insider threats. Series IAEA nuclear security series, No. 8-G (rev. 1). Vienna; 2020.

10. National nuclear security threat assessment, design basis threats and representative threat statements. Series IAEA nuclear security series, No. 10-G (Rev. 1). Vienna; 2021.

11. Kovalev M.M. Education for the digital economy. *Digital Transformation* 2018;(1):37-42. (in Russ.)

12. [The human factor and the safety of nuclear installations]. In: Proceedings of the International Conference MK-2000. Moscow, Obninsk: ONITS Prognoz; 2001. (in Russ.)

13. Abramova V.N. [Organizational psychology, organizational culture, and safety culture in nuclear energy]. Moscow, Obninsk: IG – SOTSIN; 2009. (in Russ.)

14. Safety culture, Safety series, No.75-INSAG-4, a report by the International Nuclear Safety Advisory Group, IAEA. Vienna; 1991.

15. Examples of safety culture practices, Safety reports series, No.1, IAEA. Vienna; 1997.

16. Key practical issues in strengthening safety culture, Safety series, No. INSAG-15, a report by the International Nuclear Safety Advisory Group, IAEA. Vienna; 2002.

Сведения об авторе

Лобач Дмитрий Иосифович – кандидат технических наук, гражданский государственный служащий в отставке, Департамент по ядерной и радиационной безопасности Министерства по чрезвычайным ситуациям Республики Беларусь, Минск. ORCID: 0000-0001-5512-0032; ResearcherID: HKN-7220-2023; SPIN 8838-3030. Электронный адрес: lobachd@yandex.ru

About the author

Dmitry J. Lobach, Candidate of Engineering, retired civil servant, Department on Nuclear and Radiation Safety, Ministry of Emergency Situations of the Republic of Belarus, Minsk. ORCID: 0000-0001-5512-0032; ResearcherID: HKN-7220-2023; SPIN 8838-3030. E-mail: lobachd@yandex.ru

Вклад автора в статью

Лобач Д.И. Разработан дополнительный подход для экспертного анализа безопасности технических систем в контексте количественной оценки нанесения им ущерба, основанный на методе относительного анализа количественных закономерностей для характеристик технических систем.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов