Научная статья
УДК 004;519; DOI: 10.61260/2218-13X-2024-3-98-126

МОДЕЛЬ СВЯЗНОСТИ ИНФОРМАЦИОННОЙ, ФУНКЦИОНАЛЬНОЙ И ПОЖАРНОЙ БЕЗОПАСНОСТИ ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ

Тукмачева Марина Алексеевна;
✉Шестаков Александр Викторович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉alexandr.shestakov01@yandex.ru

Аннотация. Пожарная, функциональная и информационная безопасность на опасных промышленных объектах – наиболее важные аспекты для обеспечения устойчивости производственного процесса. В отраслях с высоким риском, стандарты пожарной, функциональной и информационной безопасности систем и процессов применяются как независимые. Расширение интеллектуализации производства, а также непрерывная цифровая трансформация бизнес-процессов обусловливают актуальность взаимосвязанности обеспечения пожарной, функциональной и информационной безопасности сложных систем. Связь между пожарной, функциональной и информационной безопасностью настолько тесна, что достаточно сложно их сегментировать. Новые противоречия и конфликты могут возникать также, когда проблемы и различные аспекты безопасности рассматриваются независимо друг от друга. Поэтому вопрос о том, как интегрировать и дифференцировать пожарную, функциональную и информационную безопасность является проблемным и достаточно актуальным и требует решения. В настоящее время имеется ряд исследований и подходов по интеграции пожарной, функциональной и информационной безопасности. Рассмотрены концепция комплексной оценки рисков и интегрированная модель жизненного цикла функциональной и информационной безопасности систем. Приведены описание и предполагаемая основа достижения интеграции различных областей безопасности. Предложено комплексное применение пожарной, функциональной и информационной безопасности опасных производственных объектов рассматривать применительно к практике государственной пожарной надзорной деятельности.

Ключевые слова: пожарная безопасность, функциональная безопасность, информационная безопасность, опасные производственные объекты, государственный пожарный надзор, математическая модель комплексной безопасности

Для цитирования: Тукмачева М.А., Шестаков А.В. Модель связности информационной, функциональной и пожарной безопасности опасных производственных объектов // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 98–126. DOI: 10.61260/2218-13X-2024-3-98-126.

Scientific article

THE MODEL OF CONNECTIVITY OF INFORMATION, FUNCTIONAL AND FIRE SAFETY OF HAZARDOUS PRODUCTION FACILITIES

Tukmacheva Marina A.;
✉Shestakov Alexander V.
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉alexandr.shestakov01@yandex.ru

Abstract. Fire, functional and information security at hazardous industrial facilities are the most important aspects to ensure the sustainability of the production process. In high-risk industries, standards for fire, functional and information security of systems and processes are applied as independent. The expansion of the intellectualization of production, as well as the continuous digital transformation of business processes, determine the relevance of the interconnectedness

of fire, functional and information security of complex systems. The connection between fire, functional and information security is so close that it is quite difficult to segment them. New contradictions and conflicts can also arise when problems and various aspects of security are considered independently of each other. Therefore, the question of how to integrate and differentiate fire, functional and information security is problematic and quite relevant, which needs to be addressed. Currently, there are a number of studies and campaigns on the integration of fire, functional and information security. The concept of a comprehensive risk assessment and an integrated model of the life cycle of functional and information security systems are considered. The description and the proposed basis for achieving integration of various security areas are given. It is proposed to consider the complex application of fire, functional and information security of hazardous production facilities in relation to the practice of state fire supervision activities.

Keywords: fire safety, functional safety, information security, hazardous production facilities, state fire supervision, mathematical model of integrated safety

For citation: Tukmacheva M.A., Shestakov A.V. The model of connectivity of information, functional and fire safety of hazardous production facilities // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 3. P. 98–126. DOI: 10.61260/2218-13X-2024-3-98-126.

Введение

Обеспечение промышленной безопасности опасных производственных объектов или состояния защищенности от аварий и последствий от них должно осуществляться соизмеримо с уровнем потенциальной опасности аварий на объектах, как определено правовыми нормами Федерального закона от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов», то есть должно соответствовать классу опасности производственного объекта, включая категорию риска, применительно к пожарной опасности.

Для полной и объективной оценки противопожарного состояния объекта различной категории риска в рамках Федерального закона от 21 декабря 1994 г. № 69-ФЗ «О пожарной безопасности», органом государственного пожарного надзора согласно «Положению о федеральном государственном пожарном надзоре», введенном в действие постановлением Правительства Российской Федерации от 12 апреля 2012 г. № 290[1], организуются и проводятся плановые контрольные (надзорные) мероприятия с различным объемом действий (инспекционный визит, рейдовый осмотр, выездная проверка, документальная проверка или выборочный контроль), а также профилактические визиты.

Аварии на опасных производственных объектах чрезвычайно опасны для жизни и здоровья людей, приводят к финансовым потерям предприятий.

Пожары происходят часто и ущерб от них достаточно серьезный.

Особую опасность представляют пожары на опасных производственных объектах (ОПО), которые размещены в мегаполисах – городах с высокой плотностью населения. Количество крупных и средних производственных предприятий, например, в Москве, по состоянию на 1 января 2024 г. достигает 4 200 ед. с численностью населения более 12,5 млн чел. Динамика количества пожаров за последние пять лет, на примере Санкт-Петербурга, приведена на рис. 1, динамика количества погибших людей на пожарах за аналогичный период – на рис. 2. Вместе с тем представленная динамика не соотносит данные к влиянию и вкладу функциональной и информационной безопасности опасных производственных объектов.

[1] О федеральном государственном пожарном надзоре: постановление Правительства Рос. Федерации (вместе с «Положением о федеральном государственном пожарном надзоре») от 12 апреля 2012 г. № 290 (в ред. от 17 апр. 2024 г.).

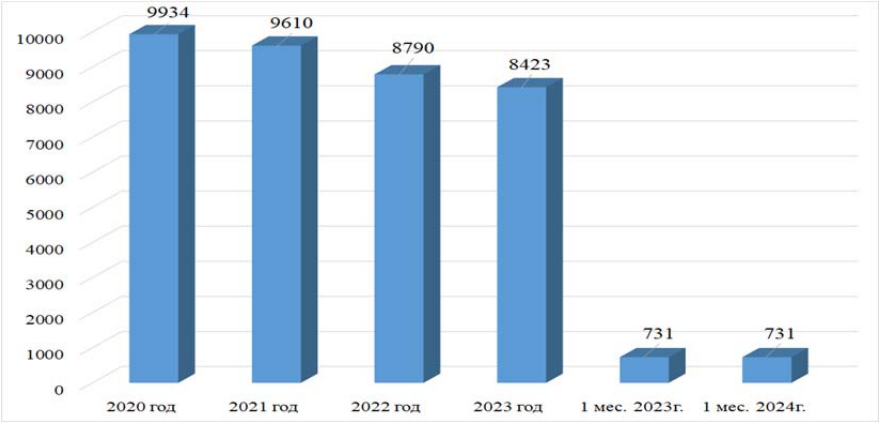

Рис. 1. **Динамика количества пожаров в Санкт-Петербурге (источник: https://78.mchs.gov.ru[2])**

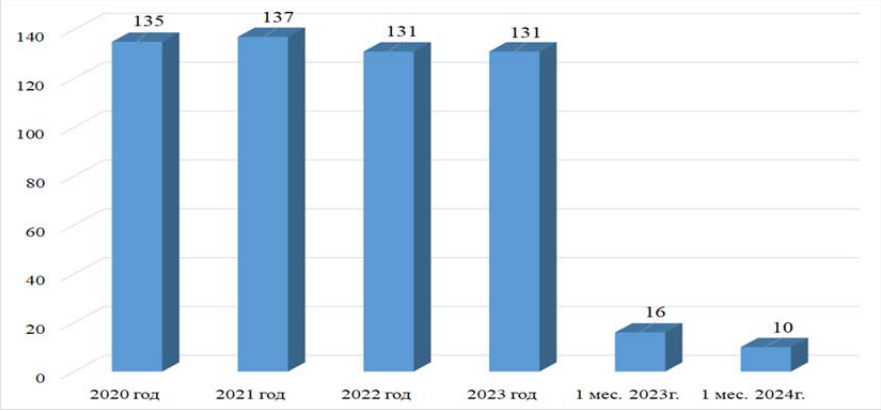

Рис. 2. **Динамика количества погибших людей на пожарах в Санкт-Петербурге (источник: https://78.mchs.gov.ru)**

Проблематика безопасности ОПО

Пожарная безопасность здания или помещения напрямую зависит от его функционального назначения. Класс функциональной пожарной опасности зданий, сооружений и пожарных отсеков, как установлено техническим регламентом, – это классификационная характеристика объектов, основанная на особенностях эксплуатации помещений, в том числе технологических процессов производства, осуществляемых в них, и обеспечении безопасности находящихся в них людей[3]. Регламентировано пять классов функциональной пожарной опасности, к одному из классов которых относят здания производственного или складского назначения. Состав и функциональные характеристики систем обеспечения пожарной безопасности производственных объектов оформляют в виде самостоятельного раздела проектной документации.

На обеспечение пожарной безопасности ОПО влияют два вида факторов:

– функциональная пожарная безопасность, которая является основой, определяющей выбор остальной противопожарной защиты;

– конструктивная пожарная безопасность.

[2] Сведения об обстановке с пожарами и их последствиями по сравнению с аналогичным периодом прошлого года. URL: https://78.mchs.gov.ru (дата обращения: 11.09.2024).

[3] Технический регламент о требованиях пожарной безопасности: Федер. закон от 22 июля 2008 г. № 123-ФЗ. Доступ из справ.-правового портала «Гарант».

Требования к объектам применяются в зависимости от назначения и способа использования ОПО, а также от степени безопасности находящихся в них людей, с учетом возраста, физического состояния, количества людей, находящихся в здании, возможности пребывания в состоянии сна. Результаты проведенного анализа нормативных документов по функциональной безопасности и документов, регламентирующих технологические процессы производства, показали, что на правила и регламенты, связанные с пожаром, приходится более 30 % всех правовых норм. Это означает, что пожар оказывает существенное влияние на безопасность ОПО.

Периодичность проведения мероприятий государственным пожарным надзором на конкретном объекте обусловливается присвоенной объекту категорией риска, показатели Q_C которого, в свою очередь, определяются исходя из ежегодных среднестатистических выборок значений вероятностных параметров возникновения пожаров P и негативных последствий U_C по аналогичной группе объектов защиты, деятельности и функциональной опасности с учетом показателя тяжести потенциальных негативных последствий пожаров $К_{г.т.}$ как степени превышения ожидаемого риска негативных последствий Q_C к допустимому $Q_{Cдоп}$:

$$Q_c = P \times U_c, \quad (1)$$

при

$$P = \frac{M_п}{Т \times M_{об}}, \quad (2)$$

$$U_c = \frac{M_г + M_т}{M_п}, \quad (3)$$

$$К_{г.т.} = \frac{Q_c}{Q_{c_{доп}}}, \quad (4)$$

где $M_п$, $M_{об}$, $M_г$, $M_т$ – количественные показатели пожаров, объектов защиты, погибших и травмированных за период мониторинга Т.

Правовыми документами предусмотрен механизм индивидуализации категории риска конкретного объекта посредством введения в общие расчетные показатели $К_{г.т.}$ дополнительного показателя $U_{инд}$ – индекса индивидуализации подконтрольного лица:

$$U_{инд} = \sum_{j=1}^{M} I_{рпв} + \sum_{i=1}^{N} I_{крд}, \quad (5)$$

где M, $I_{рпв}$ – количественные показатели и индикаторы рисков; N, $I_{крд}$ – количественные показатели и критерии добросовестности.

Это с учетом выражения (5) приводит к следующему формальному определению показателя $К_{г.т.инд}$ тяжести потенциальных негативных последствий:

$$К_{г.т.инд} = К_{г.т.} + U_{инд}. \quad (6)$$

Значение индекса $U_{инд}$ определяется органом государственного пожарного надзора по совокупности вероятностных значений индикаторов риска причинения ущерба (индивидуальных характеристик объекта).

Дополнительно к знаниям о публикуемых статистических данных состояния пожарной безопасности ОПО и причиненного ущерба следует обратить внимание на сведения о состоянии функциональной и информационной безопасности ОПО.

В отчете компании InfoWatch [4] по итогам 1 полугодия 2024 г. приведены данные об увеличении в России утечек информации на 10 % (рис. 3), в том числе в сегменте

[4] Аналитический отчет «Утечки информации в мире и России за первое полугодие 2024 года» // Экспертно-аналитический центр InfoWatch. М.: InfoWatch, 2024. 26 с.

промышленности (как следует из данных на рис. 4), при этом 99 % утечек информации обусловлена умышленными нарушениями.

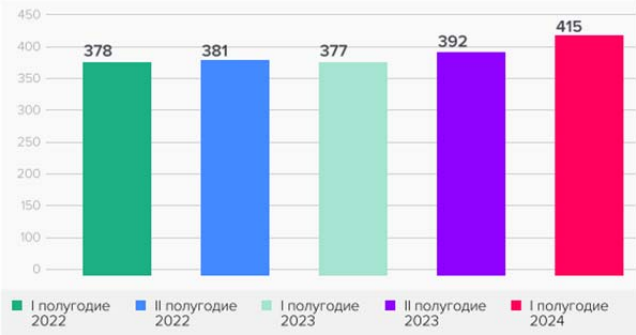

Рис. 3. **Динамика утечек информации в Российской Федерации (источник: InfoWatch)**

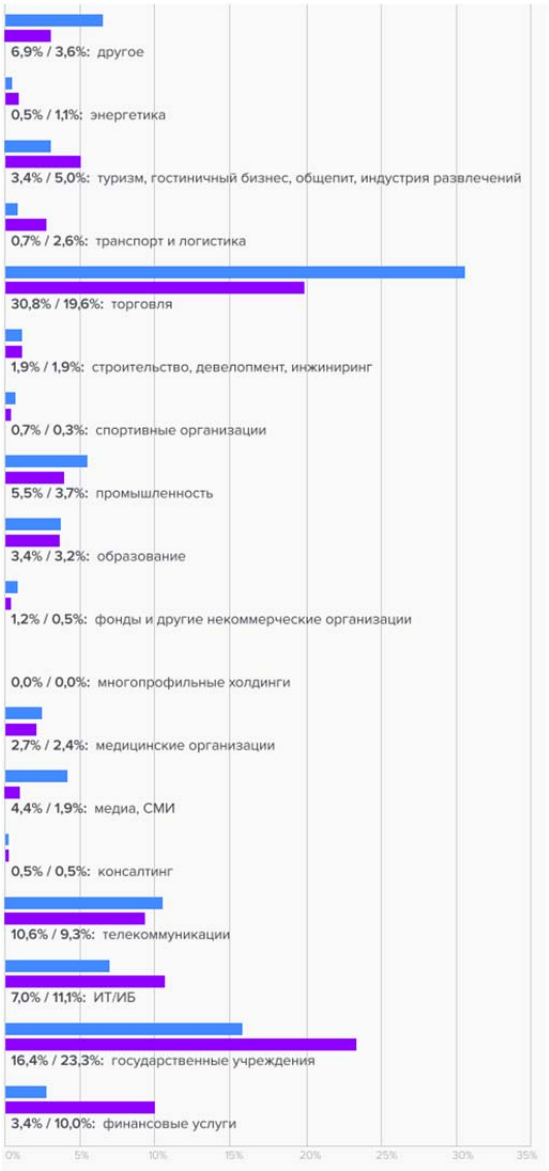

Рис. 4. **Распределение утечек информации по отраслям Российской Федерации (источник: InfoWatch)**

Детализированные данные компьютерных атак на системы управления технологическими процессами, представленные компанией InfoWatch[5], показывают, что основным каналом атак в 2023 г. является интернет с применением технологий LOTL (Living Off The Land), Golden SAML, C2 (Command and Control), VPN (Virtual Private Network), RDP (Remote Desktop Protocol), RMM (Remote Monitoring and Management), данные о которых представлены на рис. 5, а также группирование методов атак: вредоносного программного обеспечения (ВПО), изменений статуса устройств и др. (рис. 6).

Рис. 5. **Распределение каналов атак на системы управления технологическими процессами (Источник: InfoWatch)**

Рис. 6. **Распределение методов атак на системы управления технологическими процессами (АСУ ТП – автоматизированные системы управления технологическими процессами) (источник: InfoWatch)**

В отчете компании «Солар» по итогам 1 полугодия 2024 г.[6] подтвержден рост атак на АСУ ТП по нанесению предприятию максимального ущерба. Аналитики прогнозируют

[5] Тенденции развития киберинцидентов АСУ ТП за 2023 год: аналитический отчет Экспертно-аналитического центра InfoWatch. М.: InfoWatch, 2024. 21 с.

[6] Solar 4RAYS: Хроники DFIR: отчет по итогам 1 полугодия 2024. М.: Solar 4RAYS, 2024. 24 с.

на ближайшее пятилетие удвоение количества предупреждений об уязвимостях АСУ ТП при ограниченном существующем мониторинге активов информационной безопасности.

В случае внезапного появления неблагоприятных факторов и преднамеренного комплексного воздействия на различные активы опасных производственных объектов изменения, порожденные ими во вновь возникших рисках, например, функциональной и информационной безопасности, в явном виде не отражаются ни в расчетных показателях тяжести потенциальных негативных последствий (выражения (1–6), ни в изменении графика и последовательности плановых надзорных (проверочных) мероприятий государственного пожарного надзора. При этом с целью предотвращения или снижения рисков и последствий целесообразно организовать и провести на опасном производственном объекте, подвергающемуся комплексному деструктивному воздействию, мероприятия в форме профилактических.

В сложившихся условиях разработка и применение модели связности информационной, функциональной и пожарной безопасности опасных производственных объектов является достаточно востребованной задачей.

Анализ способов регулирования в области обеспечения безопасности ОПО

Расширение интеллектуализации производства, а также непрерывная цифровая трансформация бизнес-процессов во всех отраслях экономики обусловливают актуальность взаимосвязанности обеспечения пожарной, функциональной и информационной безопасности сложных систем, в частности опасных производственных объектов. Тенденции развития цифровой трансформации, формирования различных технологических платформ, внедрения искусственного интеллекта и других сквозных цифровых технологий положены в основу нового национального проекта «Экономика данных и цифровая трансформация государства», который в сентябре 2024 г. был представлен на Восточном экономическом форуме[7]. Национальным проектом предусматривает достижения прироста до 6 % показателей доходов отраслей экономики.

В сложившихся условиях в сфере обеспечения безопасности ОПО значительную роль приобретает функциональная безопасность технической основы производственных систем объектов, таких как электрические системы, электронные и программируемые (компьютерные системы), которые используются для реализации функций безопасности.

Новая парадигма безопасности, возникшая в начале XXI в., приобретает популярность с расширением интеллектуализации производственных процессов, а также непрерывной цифровой трансформацией бизнес-процессов.

Нарушение функционирования АСУ предприятием и технологическими процессами на производственных объектах может привести к техногенным и экологическим катастрофам, промышленным авариям, человеческим жертвам и значительным финансовым потерям.

В сфере отечественного нормативно-технического регулирования принята определенная группа документов, которые позиционируют «функциональную безопасность» (ФБ) с непреднамеренно вызванными отказами в выполнении отдельных функций системы. Причинами отказов в системе могут являться сбои в программе или аппаратуре, воздействие внешней среды, ошибочные действия персонала и др.

Под ФБ будем понимать часть общей безопасности системы (процессов), обеспечиваемой посредством применения специальных систем, включающих в свой состав электрические, электронные, программируемые электронные элементы, которые реализуют функции предотвращения, управления отказами и снижения рисков производственных систем.

[7] Дмитрий Григоренко представил на ВЭФ нацпроект «Экономика данных». URL: //http://government.ru/news/52567/ (дата обращения: 08.08.2024).

Для оценки компонент сложных промышленных объектов, расчет которых не регламентирован существующей нормативно-методической базой, исследователями Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики предложено использовать оригинальные численные методы и примеры расчета ФБ [1].

В 2012 г. в соответствии с изменениями в международных рекомендациях 2010 г. для систем, выполняющих функции обеспечения безопасности[8], в Российской Федерации принята и введена в действие система стандартов серии 61508[9], общая структура которых приведена на рис. 7.

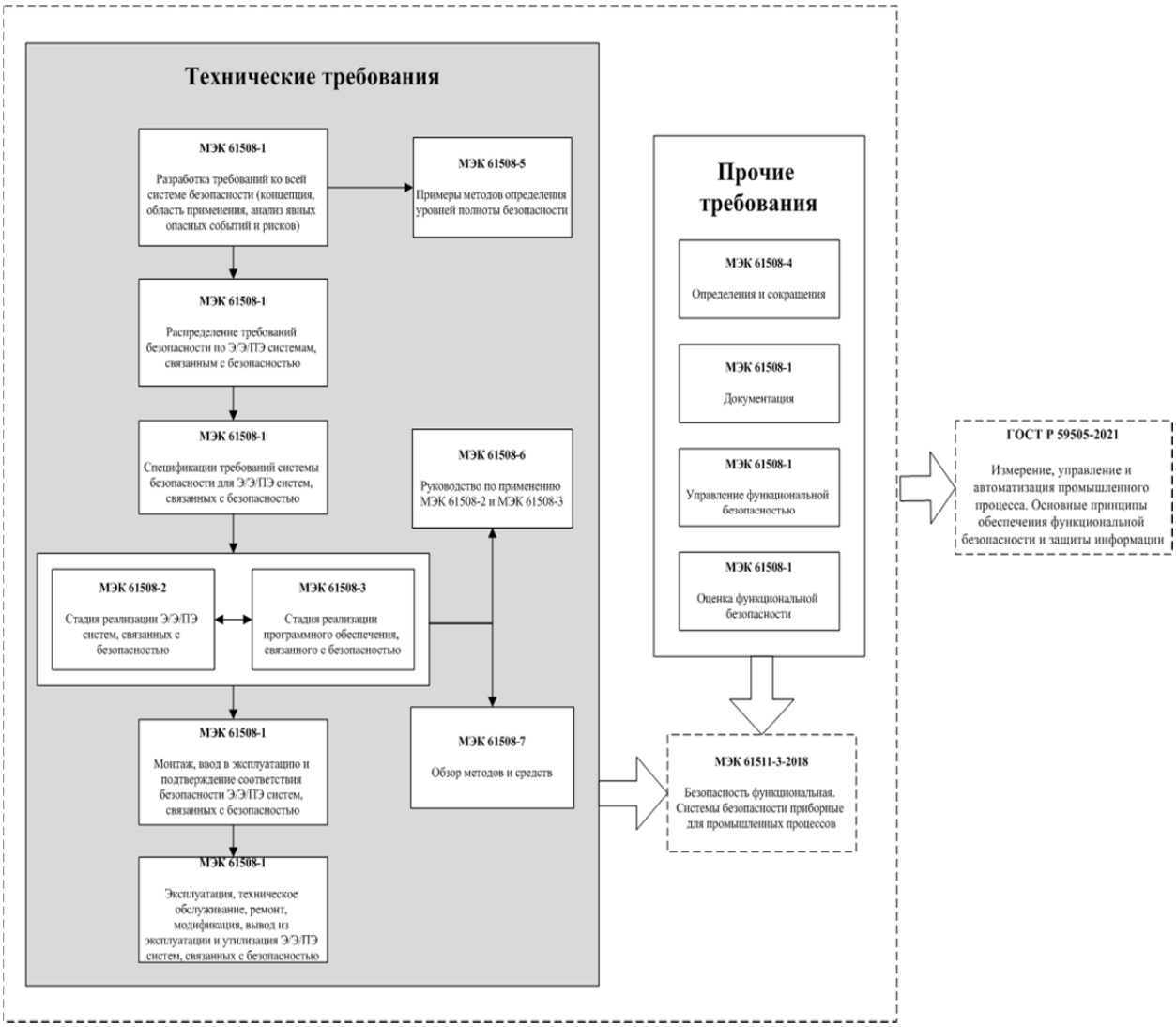

Рис. 7. **Общая структура требований стандартов МЭК серии 61508 (МЭК – Международная электротехническая комиссия) (источник: материалы ГОСТ Р МЭК 61508-1–2012)**

Национальный нормативно-технический документ МЭК серии 61508 является основным стандартом ФБ, на его основе разработаны стандарты, которые обеспечивают безопасность на опасных производственных объектах. Цель применения стандартов серии

[8] IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements.

[9] ГОСТ Р МЭК 61508-1–2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 1: Общие требования // Электронный фонд правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 05.07.2024).

61508 заключается в возможности подтверждения реализации в системе механизмов обеспечения ФБ и достаточности методов обеспечения ФБ, использованных при разработке системы[10]. При эксплуатации технологического оборудования и обеспечении безопасности на ОПО в первую очередь регламентируются функциональные системы безопасности, такие как приборная система безопасности, система защитной блокировки, система аварийного отключения.

Вместе с тем в части информационной безопасности (ИБ) причиной аварии может послужить информационная атака на активы АСУ (АСУП, АСУ ТП). Такое воздействие подвергает систему управления риску, сбою в системе и ошибкам. Например, вирус Stuxnet, при распространении посредством нерегламентированных флеш-накопителей, может заразить всю АСУ ТП и физически разрушить инфраструктуру ОПО.

Несмотря на системную полноту, сформированными стандартами МЭК серии 61508, сущностные аспекты связности функциональной безопасности и ИБ производственных объектов не только не отражены, даже не упомянуты.

Существующие стандарты ФБ и ИБ, применяемые на ОПО, должны применяться комплексно. Однако для комплексного их применения необходимо объединить существующие методы или создать новые. При комплексировании ФБ и ИБ в одну систему необходимо учитывать взаимодействия и противоречия между ФБ и ИБ в комплексной системе.

В 2016 г. МЭК установила дополнение части 3-1 рекомендаций 2010 г. серии 61508[11] к реализуемым дополнительным новым функциям безопасности существующего программного обеспечения, которые в 2019 г. были гармонизированы в отечественной системе стандартизации в виде ГОСТ Р 58489–2019 [12].

В этот же период МЭК принял ряд рекомендаций серии 61511[13] для технологических процессов в промышленности в части приборных систем безопасности, которые в рамках процесса гармонизации национальной системы стандартизации были приняты и введены в действие как ГОСТ Р МЭК 61511[14] в 2018 г., в основе которых положены концепция жизненного цикла системы безопасности и уровней полноты безопасности применительно к процессам, то есть конкретизации общих подходов изложенных в серии МЭК 61508 (2010).

Методическая часть документа содержит методы оценки различных опасностей, рисков и определения «уровня полноты безопасности» (УПБ):

– полуколичественный метод (анализ дерева событий);

– метод матрицы слоев безопасности;

– полукачественный метод с калиброванным графом рисков;

– качественный метод с графом рисков;

– метод анализа слоев защиты.

Структура документов серии 61511 представлена на рис. 8.

[10] Функциональная безопасность компьютерных систем управления. Ч. 8: Методы обеспечения информационной и функциональной безопасности. URL: https://www.securitylab.ru/analytics/487450.php/?ysclid=m0v3ient4v523640673 (дата обращения: 05.07.2024).

[11] IEC/TS 61508-3-1:2016 «Functional safety of electricab'electronic, «programmable electronic safety-related systems. Part 3-1: Software requirements – Reuse of pre-existing software elements to implement all or part of a safety function», IDT.

[12] ГОСТ Р 58489–2019/IEC/TC 61508-3-1. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 3-1: Требования к программному обеспечению. Повторное использование уже существующих элементов программного обеспечения для реализации всей или части функции безопасности.

[13] IEC 61511-1:2016. Functional safety – Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and application programming requirements.

[14] ГОСТ Р МЭК 61511-3–2018. Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Ч. 3: Руководство по определению требуемых уровней полноты безопасности.

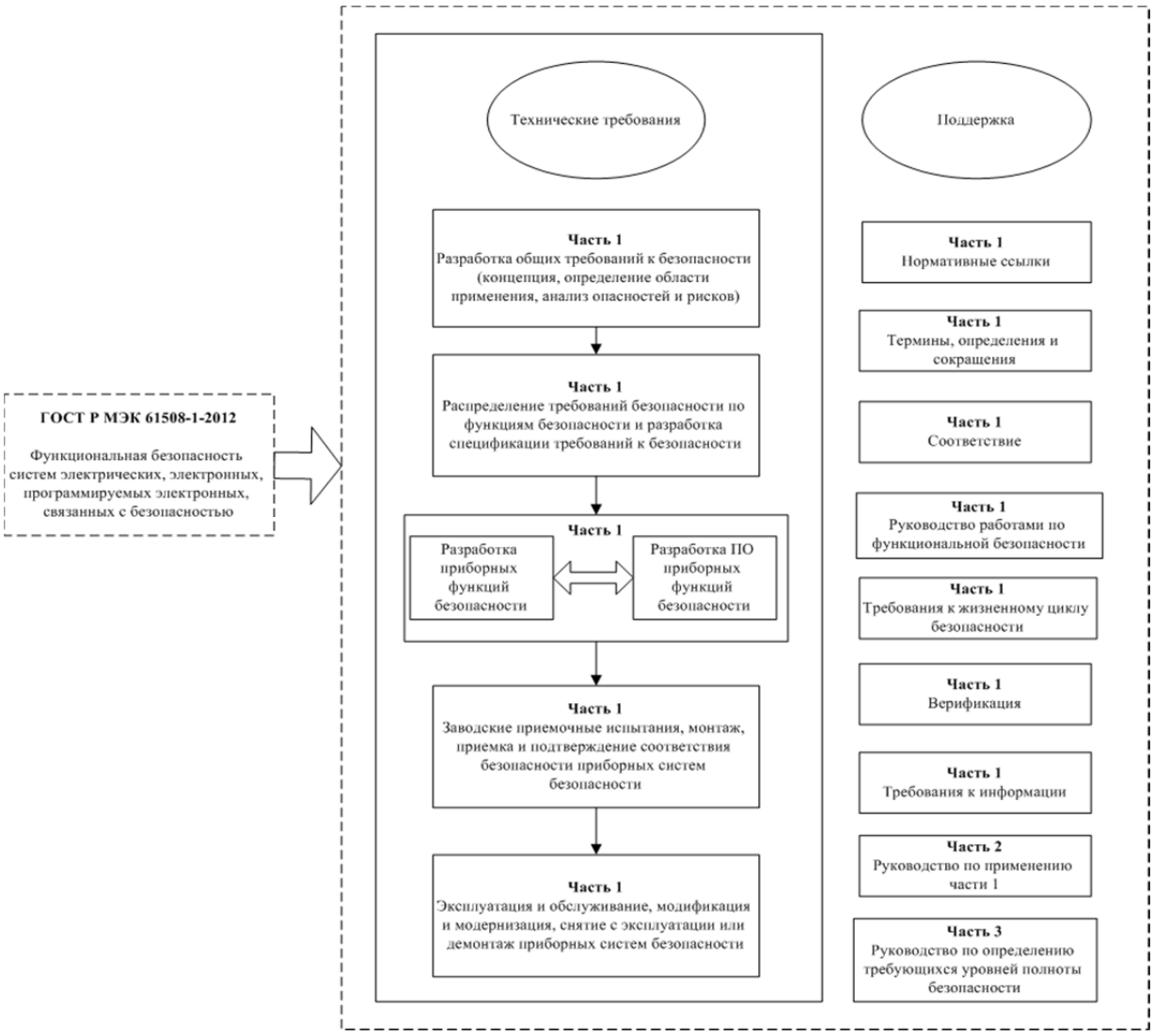

Рис. 8. **Общая структура требований стандартов МЭК серии 61511 (ПО – программное обеспечение) (источник: материалы ГОСТ Р МЭК 61511-3–2018)**

Методическому аппарату оценки показателей ФБ систем противоаварийной защиты ОПО посвящен ряд публикаций нескольких групп отечественных исследователей, в которых рассмотрены особенности построения систем защиты [2] и оценки показателей ФБ [3], комплекс методов расчета [4], в том числе методов решения прямой и обратной задачи [5], вероятности и средней наработки до ложного срабатывания [6].

Период с 2009 по 2016 г. характеризовался различными результатами гармонизации международных рекомендаций МЭК серии 62443[15]в области ИБ систем промышленной автоматики и контроля (Industrial Automation and Control Systems, IACS[16]) в отечественные

[15] IEC/TS 62443-1-1:2009 «Industrial communication networks – Network and system security. Part 1-1: Terminology, concepts and models».

[16] Компоненты, относящиеся к IACS, согласно требованиям п. 1.3 ГОСТ Р 56205–2014 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1: Терминология, концептуальные положения и модели», относятся: распределенные системы управления (Distributed Control System, DCS), программируемые логические контроллеры (Programmable Logic Controller, PLC), пульты дистанционного управления (Remote Terminal Unit, RTU), интеллектуальные электронные устройства, системы SCADA (Supervisory Control and Data Acquisition), объединенные системы электронного детектирования и контроля, системы учета и сдачи-приемки, а также системы мониторинга и диагностики, которые наделены базовыми функциями систем управления процессами и автоматизированных систем безопасности (Safety-Instrumented System, SIS), которые могут быть, как физически отделены друг от друга, так и объединены друг с другом.

стандарты, практическая реализация компонент которых встречается в сетях распределения электроэнергии, газа, воды, системах нефте- и газодобычи и нефтепродуктопроводов. Отечественные стандарты серии 62443[17] приняты в 2016 г. и введены в действие в 2017 г., регламентируют требования безопасности промышленных систем и сетей коммуникации. Общая структура требований стандартов серии 62443 представлена на рис. 9.

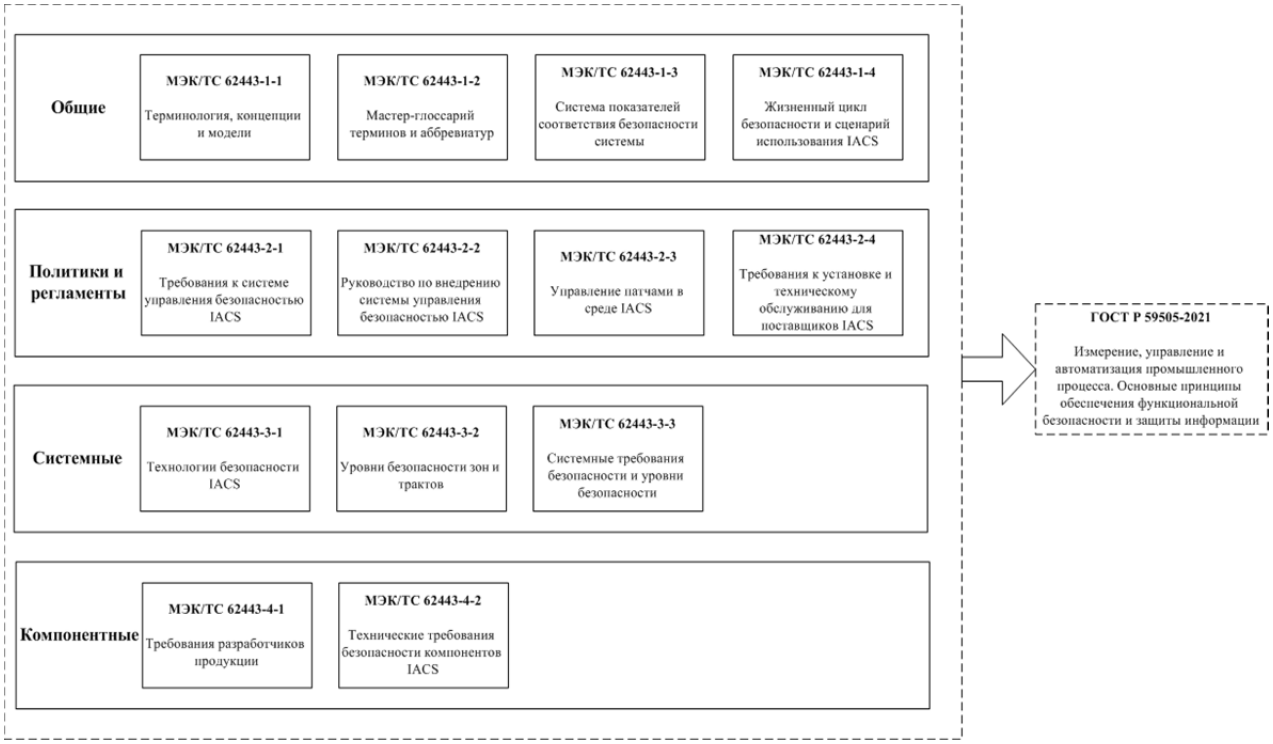

Рис. 9. **Общая структура отечественных стандартов серии 62443 (источник: материалы ГОСТ Р МЭК 62443-3-3–2016)**

При обеспечении промышленной ИБ учитывается доступность системы и ее частей. Указывается, что требования обеспечения ИБ промышленных систем не могут быть заимствованы из стандартов в области информационных систем и информационных технологий.

В 2014 г. принят и введен в действие в Российской Федерации с 2016 г. ГОСТ Р 56205, который регламентирует защищенность (кибербезопасность) сетей и систем промышленной автоматики и контроля. ИБ применительно к системам промышленной безопасности в отличие от информационных и компьютерных систем обладает иной иерархией приоритетов «доступности», «целостности» и «конфиденциальности», а также набора базовых требований к доступности ресурсов, управлению доступом, контролю использования, целостности и конфиденциальности данных, ограничению потока данных и своевременности реагирования на событие. Предполагается в перспективе интеграция кибербезопасности систем промышленной автоматики и контроля с ИБ информационных (компьютерных) систем (рис. 10).

[17] ГОСТ Р МЭК 62443-3-3–2016. Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности // Электронный фонд правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 05.07.2024).

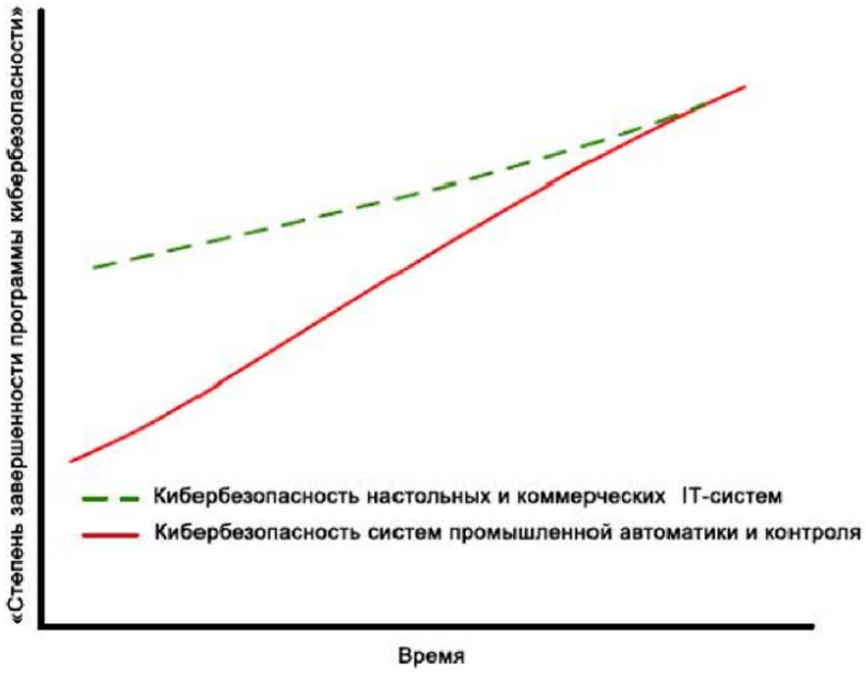

Рис. 10. **Тенденция интеграции кибербезопасности с ИБ**

Документом регламентировано понятие «риск» как «ожидание ущерба». Это вероятностная характеристика P того, что i-й источник угрозы воспользуется j-й уязвимостью объекта для достижения отрицательных m-последствий. В перечень рисков могут входить риски для: безопасности персонала (смерть, травмы); технологической безопасности (повреждение оборудования или сбои бизнес-процесса); ИБ (финансовые, правовые и т.п.); экологические (уведомления о нарушении, правовые нарушения и значительный ущерб).

Методика его оценки по задействованным системам (от непосредственно доступных для угрозы) поэтапная:

– оценка риска до реализации мер защиты или контрмер (исходного);

– реализация мер защиты или контрмер по смягчению риска;

– оценка остаточного риска.

Заслуживает особого внимания принципиальная трактовка документа в части совмещения рисков ИБ с другими рисками, что «безопасность IACS не привносит новых рисков, а требует переосмысления способа определения уровня допустимости риска, связанного с ИБ».

В 2019 г. МЭК приняла рекомендации серии 63069 в области измерения, управления и автоматизации промышленного процесса в части обеспечения ФБ и защиты информации, которые отражены в аналогичном отечественном стандарте ГОСТ Р 59505–2021[18], цель которого разъяснение и рекомендации по применению стандартов серии 61508 и 62443 в иной области применения с учетом имеющихся разнородных терминологических расхождений и трактовок, например, «безопасность», «защита», «риск» и др.

В 2020 г. МЭК приняла рекомендации серии 63325, учитывающие требования к системам контроля промышленной автоматизации на различных этапах жизненного цикла, применительно к ФБ и защите информации[19], которые в Российской Федерации в рамках гармонизации нормативно-правовой базы в 2024 г. приняты и введены в действие как

[18] ГОСТ Р 59505–2021. Измерение, управление и автоматизация промышленного процесса. Основные принципы обеспечения функциональной безопасности и защиты информации. // Электронный фонд правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 05.07.2024).

[19] IEC/PAS 63325:2020 «Lifecycle requirements for functional safety and security for IACS», IDT.

ГОСТ Р 71452[20]. Особенностью положений документа является изложение компромиссных решений в системах управления и управляемого оборудования промышленной автоматизации по предупреждению и разрешению конфликтов между функциями обеспечения ФБ и применяемыми контрмерами защиты информации. Регламентированный процесс оценки рисков представлен на рис. 11.

Рис. 11. **Процедуры оценки рисков ФБ и защиты информации IACS (источник: ГОСТ Р 71452–2024)**

Особенности организации гармонизации с международными рекомендациями (рис. 12) требований национальных стандартов в области ИБ и ФБ объектов, применительно к железнодорожному транспорту Республики Беларусь, в том числе в условиях электромагнитных влияний и терроризма, рассмотрены в работе [7] на основе двухмерной модели кибербезопасности (рис. 13).

[20] ГОСТ Р 71452–2024/IEC/PAS 63325:2020. Требования к функциональной безопасности и защите системы контроля промышленной автоматизации (IACS) на протяжении жизненного цикла. // Электронный фонд правовой и нормативно-технической документации. URL: http://www.docs.cntd.ru (дата обращения: 05.07.2024).

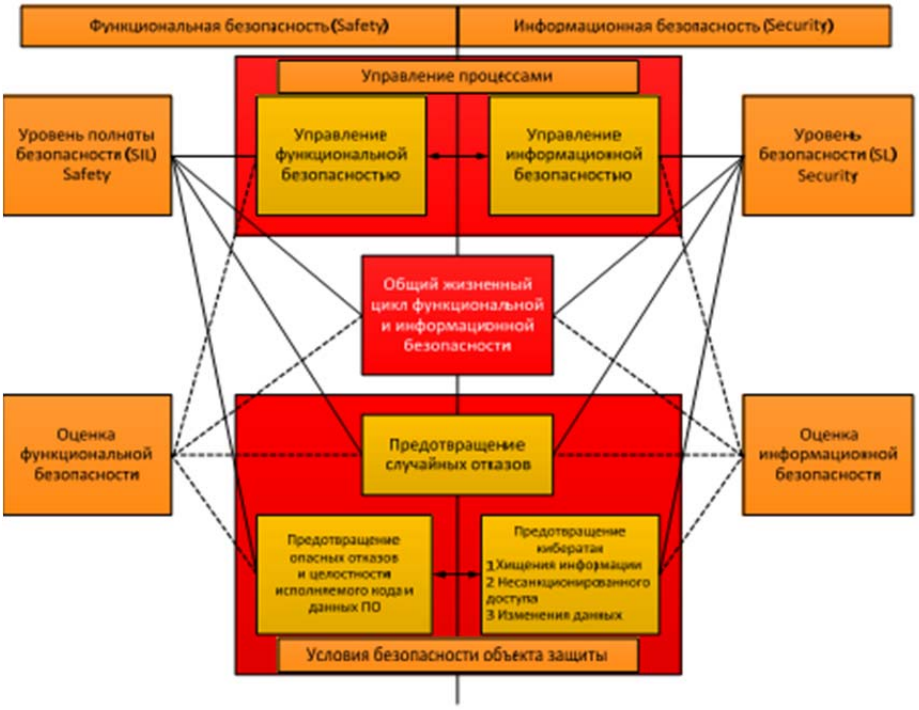

Рис. 12. **Гармонизация требований ИБ и ФБ отраслевой АСУ [7]**

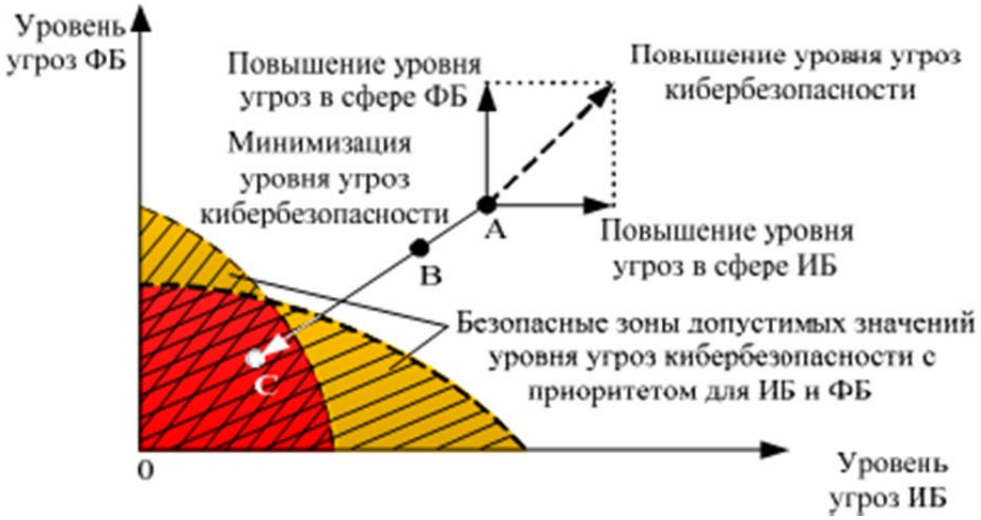

Рис. 13. **Модель кибербезопасности отраслевой АСУ [7]**

Связность ИБ, ФБ и пожарной безопасности ОПО

Новое понимание необходимости комплексного системного исследования ФБ и кибербезопасности промышленных систем и выработки новых системных подходов к совместной оценке безопасности и рисков стало основным фактором появления научных публикаций с результатами работ зарубежных и отечественных ученых и специалистов. Сведения о динамике потока публикаций по запросу «функциональная безопасность и кибербезопасность» представлены данными информационной системы academia.edu[21], которые отражены на рис. 14.

[21] URL: https://www.academia.edu.

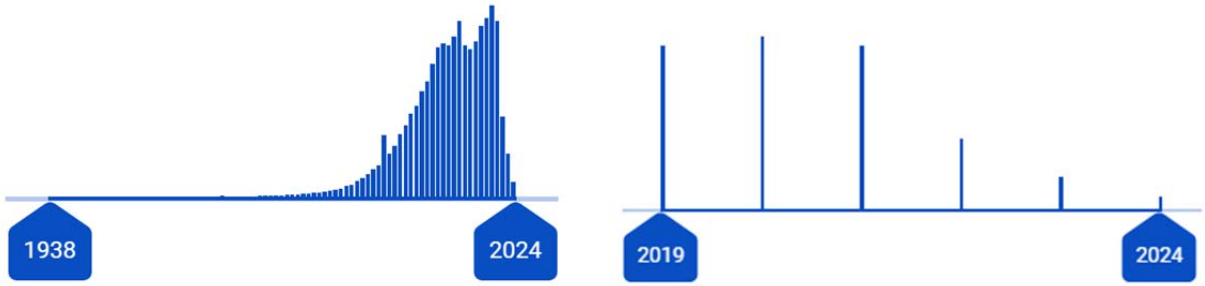

Рис. 14. **Общий объем публикаций 447 142 ед. и 233 787 ед. за последние пять лет**

Описание комплексного применения ИБ и ФБ в работе [8]. Проведено сравнение двух жизненных циклов систем, результаты которого показывают, что ФБ и ИБ следуют основным принципам оценки рисков, защиты безопасности, эксплуатации и обслуживания. Для общей системы оба жизненных цикла применимы, однако необходимо учитывать проблемы взаимодействия между ними. Блок-схемы, соответствующие фазам двух жизненных циклов и представленные на рис. 15–17, показывают связанные процессы.

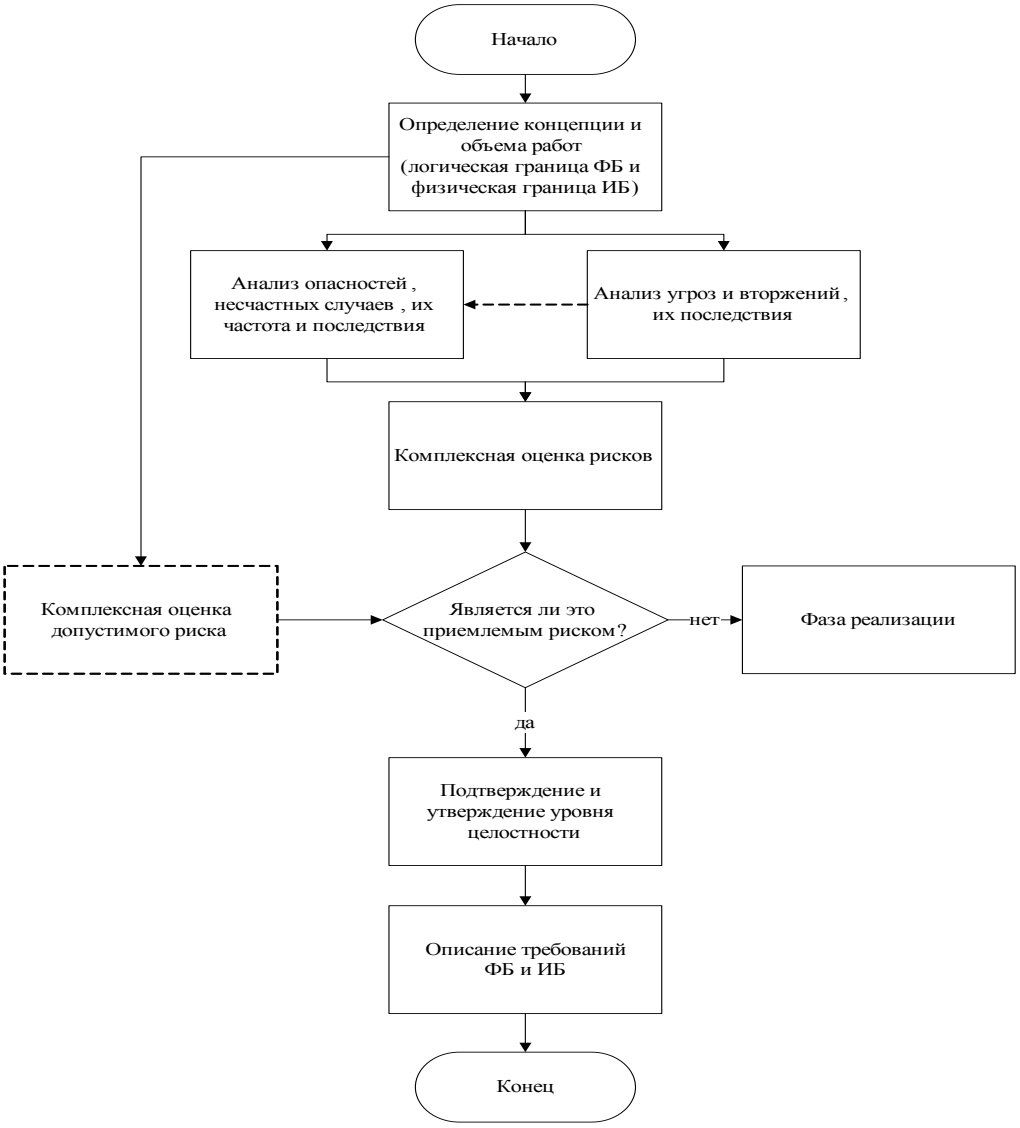

Рис. 15. **Этап модели-оценки жизненного цикла интеграции безопасности [8]**

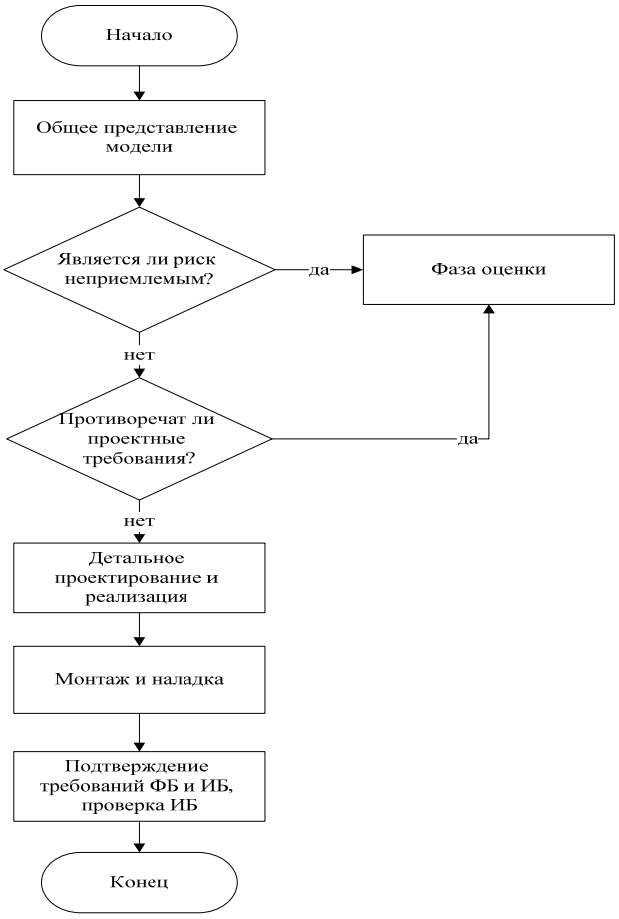

Рис. 16. **Этап модели-реализации жизненного цикла интеграции безопасности [8]**

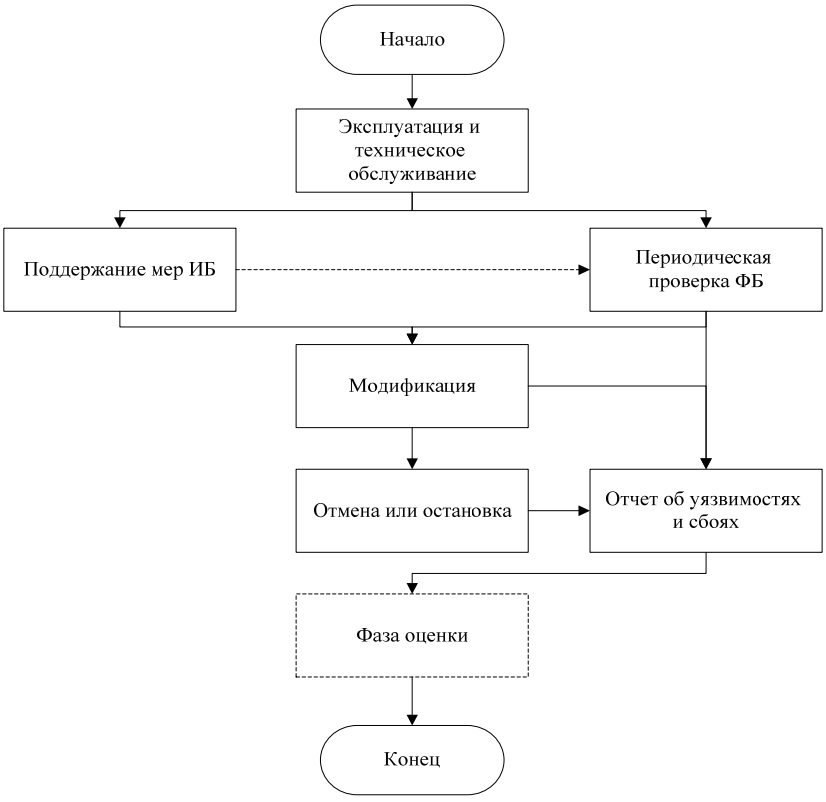

Рис. 17. **Этап модели-эксплуатации и технического обслуживания жизненного цикла интеграции безопасности [8]**

Информационно-логические связи между ФБ и ИБ в соответствии с работой [8] показаны на рис. 18.

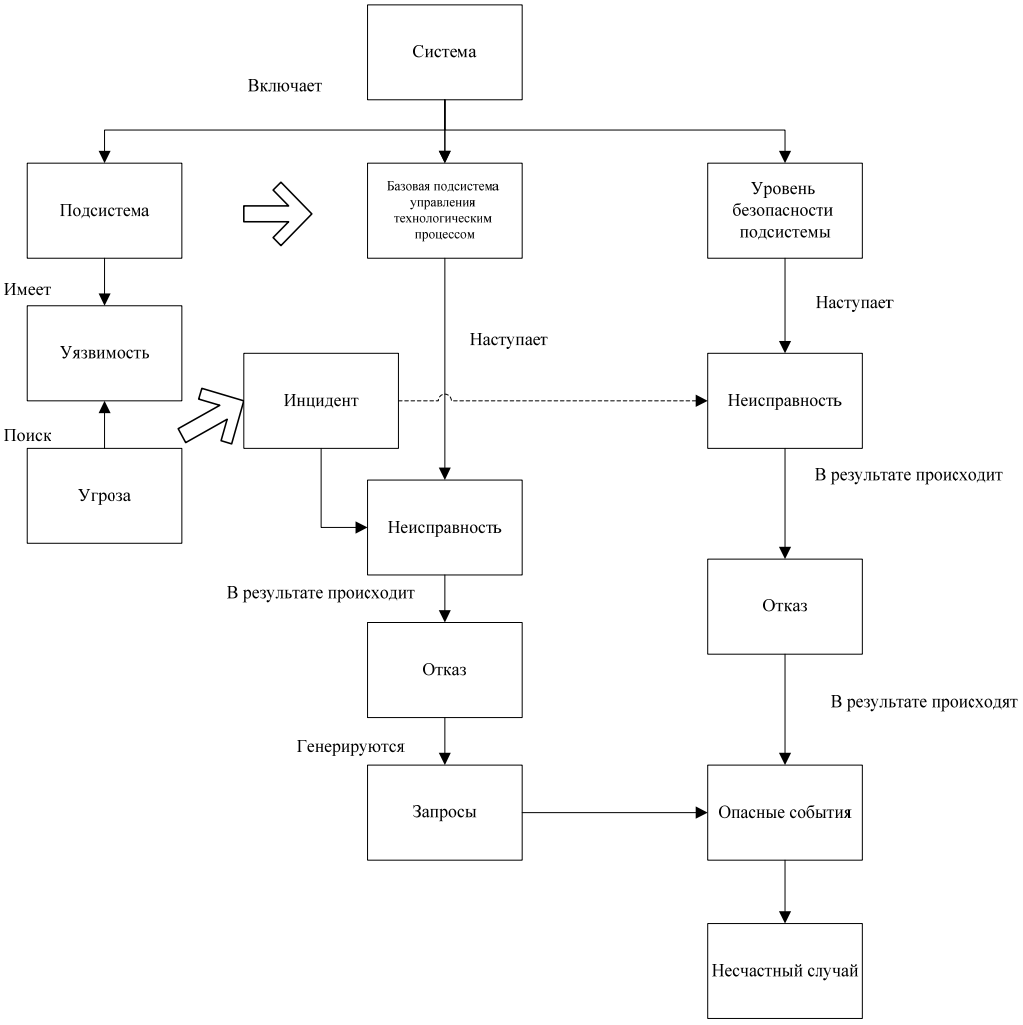

Рис. 18. **Информационно-логические связи на системном уровне между ФБ и ИБ [8]**

В аспекте организации ФБ система разделена на подсистему, связанную с безопасностью, и базовую подсистему управления процессом. Отказ базовой подсистемы управления процессом приведет к запросу системы безопасности, следовательно, обе подсистемы могут иметь проблемы с ИБ. Поскольку проблемы могут воздействовать из окружающей среды, во время работы в системе, связанной с безопасностью, возникает неисправность. В случае, если неисправность не устраняется (например, отказоустойчивость), может произойти сбой или отказ в системе. Если запросы генерируются (для системы, находящейся в режиме запроса) или система находится в непрерывном режиме в это время, будут происходить опасные события, вызывающие несчастные случаи или наносящие ущерб людям, имуществу или окружающей среде.

В аспекте организации ИБ уязвимость может быть в любой подсистеме. Если угрозы обнаружат эту уязвимость и выполнят атаки, произойдет инцидент защиты информации. Этот инцидент может привести к трем последствиям: возникновение других инцидентов без какого-либо влияния на безопасность; если этот инцидент происходит в основной подсистеме управления процессом, он станет новым источником неисправности; если этот инцидент происходит в системе, связанной с безопасностью, он также станет новым источником неисправности [8].

В работе [9] комплексно рассмотрены ФБ и кибербезопасность, представлены результаты их комплексного анализа применительно к производственным системам, которые послужили основой для продолжения исследований и их развития в работах [10, 11].

По результатам анализа способов регулирования показателей обеспечения безопасности ОПО и некоторых аспектов формирования системы показателей ИБ, ФБ и пожарной безопасности объектов либо на основе их группирования в соответствии с реализуемыми процедурами, что приводит к процедурно-связанным параметрам, либо на основе временных диапазонов их случайного возникновения, что приводит к вероятностно-временному их представлению, либо на основе логической связи в рамках определенного события, что приводит к необходимости представлению не только функций, а также и разнородных наборов данных, выявлена необходимость введения новой сущности отношений между ИБ, ФБ и пожарной безопасностью объектов, такой как «связность».

Примеры подобного использования термина «связность» имеют место в моделировании (описания бизнес-процессов: нотации стандарта IDEF0 (ICAM Definition) 1981 г.), в телекоммуникациях (в 1999 г. регламентирована система показателей IPPM Metrics for Measuring Connectivity для характеристики и измерения связности стандартным протоколом (Internet Official Protocol Standards, STD 1) сети Internet); в математике (для описания отношений между объектами в сформулированных условиях: аффинная связность в Символах Кристоффеля (Леви-Чивиты); в экономике (процедуры анализа структуры отношений и связей отраслевой системы на основе матричных балансовых моделей); в добывающих отраслях (методы перколяции (условно – «геометрическая связность») и гидродинамической связности).

Под «связностью ИБ, ФБ и пожарной безопасности опасных производственных объектов» будем понимать «способы, методы и форму представления структуры отношений и связей регламентированного обеспечения ИБ и ФБ с пожарной безопасностью объектов».

Связность ИБ, ФБ и пожарной безопасности ОПО будем рассматривать с учетом следующих положений:

а) в части ФБ проводить оценку рисков, случайные и неслучайные причины оценивать как статистические сбои;

б) в части ИБ проводить оценку рисков-угроз, неслучайные причины оценивать с применением динамических сценариев уязвимостей, которые определять как недостатки технологий, процессов, процедур или персонала, не отождествлять со сбоями, отказами и ошибками в системах;

в) показатели уровня полноты ФБ (SIL, Safety Integrity Level) и ИБ (SL, Security Level) считать независимыми, коррелированность отсутствует.

Расчет комплекса показателей, которые необходимы для определения УПБ средствами противоаварийной автоматической защиты (ПАЗ), осуществляется, как правило, на основе иерархической двухуровневой математической модели, например, представленной Российским государственным университетом нефти и газа имени И.М. Губкина [12, 13]:

– на первом – расчет частных показателей (интенсивности отказа и интенсивности ложных срабатываний ПАЗ с учетом ее архитектуры);

– на втором – расчет комплекса показателей безопасности системы ПАЗ с учетом взаимодействия с технологическим блоком ОПО и методов укрупнения состояний системы ПАЗ.

Программная реализация процедур назначения уровня полноты ФБ УПБ/SIL достаточно широко распространена. Например, известен зарегистрированный в Роспатенте в 2022 г. программный комплекс «SILATIS»[22] для ОПО, который назначает контуру

[22] Свидетельство на программу для ЭВМ «Программный комплекс «SILATIS» для автоматизированного ввода данных, выполнения вычислений и документирования результатов при проведении риск-сессий «Анализ опасностей и работоспособности (АОР) и оценка рисков с назначением уровней полноты безопасности (УПБ/SIL) приборным контурам безопасности опасных производственных объектов», ПК «SILATIS» от 14 окт. 2022 г., № 2022669001. Бюл. № 10. Правообладатель: ООО «Специализированная инжиниринговая компания Севзамонтажавтоматика».

приборных систем безопасности (ПСБ) УПБ/SIL по результатам анализа опасностей, работоспособности (АОР), то есть частоты и последствий опасных событий, и оценки рисков с учетом распределения по слоям защиты требуемого снижения риска (от вероятности инициализирующей причины до максимально допустимого (приемлемого) значения вероятности опасного события (TMEL). Перечень реализованных процедур содержит: HAZOP (АОР), LOP A/SIL (Анализ слоев защиты (АСЗ)/Назначение SIL), HAZOP SIS (АОР ПСБ); ввода данных и характеристик SIF, выпуск таблиц-отчетов согласно спецификации требований к безопасности (SRS) ПСБ.

В 2023 г. зарегистрирован в Роспатенте программный комплекс HazOps[23], который обеспечивает проведение АОР независимых слоев защиты контуров безопасности систем ПАЗ и достаточности мер безопасности с назначением УПБ/SIL. Известна также программа автоматизированной подготовки данных HAZOP SIS[24], которая обеспечивает формирование рабочей таблицы HAZOP SIS по результатам АОР (HAZOP) и SIL-анализа посредством анализа в специальной базе данных содержания таблиц HAZOP/SIL, поиска данных по функциям безопасности контуров ПАЗ, группирования их по функциям и занесения в таблицу HAZOP SIS.

Формальная математическая модель описания уровня полноты функциональной безопасности (УПБф) или Safety Integrity Level (SIL) представлена в виде матрицы, элементы которой содержат оценки (показатели) УПБф по каждой n-й подсистеме и m-й функции:

$$[\text{УПБф}]_{n\times m} = \begin{bmatrix} \text{УПБф}_{11} & \dots & \text{УПБф}_{1m} \\ \dots & \dots & \dots \\ \text{УПБф}_{n1} & \dots & \text{УПБф}_{nm} \end{bmatrix}$$

или

$$[\text{SIL}]_{n\times m} = \begin{bmatrix} \text{SIL}_{11} & \dots & \text{SIL}_{1m} \\ \dots & \dots & \dots \\ \text{SIL}_{n1} & \dots & \text{SIL}_{nm} \end{bmatrix}.$$

Формальная математическая модель описания уровня полноты информационной безопасности (УПБи) или Security Level (SL) может быть представлена в виде матрицы, элементы которой содержат оценки (показатели) УПБи по каждой n-й подсистеме и m-й функции:

$$[\text{УПБи}]_{n\times m} = \begin{bmatrix} \text{УПБи}_{11} & \dots & \text{УПБи}_{1m} \\ \dots & \dots & \dots \\ \text{УПБи}_{n1} & \dots & \text{УПБи}_{nm} \end{bmatrix}$$

или

$$[\text{SL}]_{n\times m} = \begin{bmatrix} \text{SL}_{11} & \dots & \text{SL}_{1m} \\ \dots & \dots & \dots \\ \text{SL}_{n1} & \dots & \text{SL}_{nm} \end{bmatrix}.$$

Формальная математическая модель связности ИБ, ФБ и пожарной безопасности представлена в виде матрицы УПБо уровня полноты безопасности объекта на основе матриц УПБи и УПБф:

[23] Свидетельство на программу для ЭВМ «HazOps (программный комплекс по анализу опасностей и работоспособности с назначением целевого уровня полноты безопасности на опасных производственных объектах» от 9 февр. 2023 г., № 2023612931. Бюл. № 2. Правообладатель: ООО «Эр Би Ай Концепт».

[24] Свидетельство на программу для ЭВМ «Программа автоматизированной подготовки исходных данных HAZOP SIS (ПК «HAZOP SIS»)» от 23 мая 2023, № 2023660659. Бюл. № 6. Правообладатель: ООО «НТЦ «ТБ».

$$[\text{УПБо}]_{n\times m} = [\overline{\text{УПБи}}]_{n\times m} \times \left[\overline{\text{УПБф}}\right]_{n\times m},$$

в итоговом виде:

$$[\text{УПБо}]_{n\times m} = \begin{bmatrix} \text{УПБо}_{11} & \dots & \text{УПБо}_{1m} \\ \dots & \dots & \dots \\ \text{УПБо}_{n1} & \dots & \text{УПБо}_{nm} \end{bmatrix}.$$

По результатам анализа зарегистрированных программ для ЭВМ и баз данных в области мониторинга ФБ и ИБ за последние пять лет выявлено 102 результата, характеристики наиболее значимых из которых, несмотря на имеющие ограничения и недостатки для целей настоящего исследования, сведены в табличную форму (табл. 1).

Таблица 1

Характеристики программных средств с функциями обеспечения ИБ и ФБ промышленных объектов

Перечень характеристик	Программные средства		
	№ 2021619813	№ 2024613304	№ 2024680211
Наименование	Система автоматизированного мониторинга и контроля промышленной безопасности гидротехнических сооружений (ГТС)	Платформа распределенной корреляции событий промышленных информационных систем с обогащением данных из неструктурированных источников для сервиса мониторинга и реагирования на инциденты	Система автоматизации реагирования на инциденты ИБ SECAI AIR
Функции	1. Сбор данных измерительного оборудования ГТС. 2. Отображение данных	1. Сбор и унификация данных в БД. 2. Сбор дополнительных данных об объекте, событиях ИБ, проверок, анализа атак. 3. Выявление аномалий на основе исторического профилирования и статистического анализа	1. Сбор событий и инцидентов ИБ из внешних систем. 2. Опрос неинтегрируемых систем. 3. Проверка правил реагирования. 4. Запуск сценария реагирования
Дата создания	17.06.2021 г.	09.02.2024 г.	27.08.2024 г.
Разработчик	ООО «Центр исследований экстремальных ситуаций»	ООО «Инфосекьюрити»	ООО «Секай»

Предложенный подход, основанный на модели связности ИБ, ФБ и пожарной безопасности, позволяет организовать более адекватный и достоверный мониторинг состояния системы безопасности ОПО, реализованной в соответствии с современными регламентированными взаимоувязанными комплексами требований к информационной, функциональной и пожарной безопасности ОПО. В качестве примера традиционных подходов можно привести зарегистрированное Роспатентом программное средство непрерывного мониторинга (№ 2021616445 от 21 апреля 2021 г.)[25], которое в реальном масштабе времени предоставляет текущие расчетные данные мониторинга систем противопожарной защиты и результаты подсчета количества людей, которые определяют

[25] Свидетельство на программу для ЭВМ «Информационная система непрерывного мониторинга пожарного риска в здании» от 21 апр. 2021 г., № 2021616445. 21.04.2021. Бюл. № 5/ Правообладатель: Шихалев Д.В.

величину пожарного риска объекта, на основании которого осуществляется последующий расчет эвакуации людей посредством моделирования их движения (в частности, индивидуально-поточного).

Представленный выше материал отражает методологические подходы и регламентированные процедуры по формированию требуемого уровня ИБ, ФБ и пожарной безопасности применительно к производственным объектам и процессам, а также к системам (средствам) управления ими, однако подходы и технологии по их мониторингу и своевременному выявлению аномалий не отражены. Вместе с тем раннее предупреждение об аномалиях дает возможность избежать опасных отказов и инцидентов защиты информации[26].

Следовательно, актуальной прикладной задачей для государственного пожарного надзора является соизмеримость профилактических мероприятий с уровнем аномалий значений показателей ФБ и ИБ, увязанных с пожарной безопасностью ОПО.

Применение модели связности ИБ, ФБ и пожарной безопасности объектов в деятельности государственного пожарного надзора

Организация профилактических мероприятий государственного пожарного надзора на основе модели связности содержит несколько укрупненных блоков:

– Сбор, обработка данных от государственных информационных систем применительно к конкретному ОПО, который подвергается контролю. Характеристики типовых информационных ресурсов (систем) представлены в табл. 2.

Таблица 2

Характеристики информационных ресурсов (систем) с данными об ОПО

Информационные ресурсы	Перечень характеристик			
	наименование	сервисы	оператор	примечание
ГИС АИУС РСЧС	Государственная информационная система «Автоматизированная информационно-управляющая система единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций»	Геоинформационная система База знаний База аналитики Данные дистанционного зондирования Земли Атлас опасностей и рисков Паспорт территорий Термические точки Информационно-аналитическая система	МЧС России	Постановление Правительства Российской Федерации от 24 января 2024 г. № 57
ААС КЕЛ	Информационная система «Автоматизированная аналитическая система поддержки управления контрольно-надзорными органами	Реестр поднадзорных объектов. Реестр собственников. Реестр контрольных (надзорных) мероприятий. Реестр административных дел. Реестр профилактики. Реестр изменений	МЧС России (ФГБУ ИАЦ МЧС России)	Приказ МЧС России от 4 октября 2022 г. № 954

[26] URL: https://hsseworld.com/introduction-to-process-safety-indicators-free-guide-for-measuring-performance-2. URL: https://www.safetyinfo.com/process-safety-management-elements-psm-free-index.

Информационные ресурсы	Перечень характеристик			
	наименование	сервисы	оператор	примечание
	МЧС России»	категорий рисков. Реестр подразделений и должностных лиц. Модуль учета пожаров и их последствий. Модуль мониторинга		

– Сбор, обработка данных удаленного мониторинга от систем ПАЗ, приборных систем безопасности (ПСБ) и других подсистем ИБ и ФБ ОПО, который подвергается контролю с целью формирования исходных данных требуемого перечня и полноты, для проведения последующего анализа с применением цифровых технологий больших данных.

Возможный набор данных IACS представлен на рис. 19.

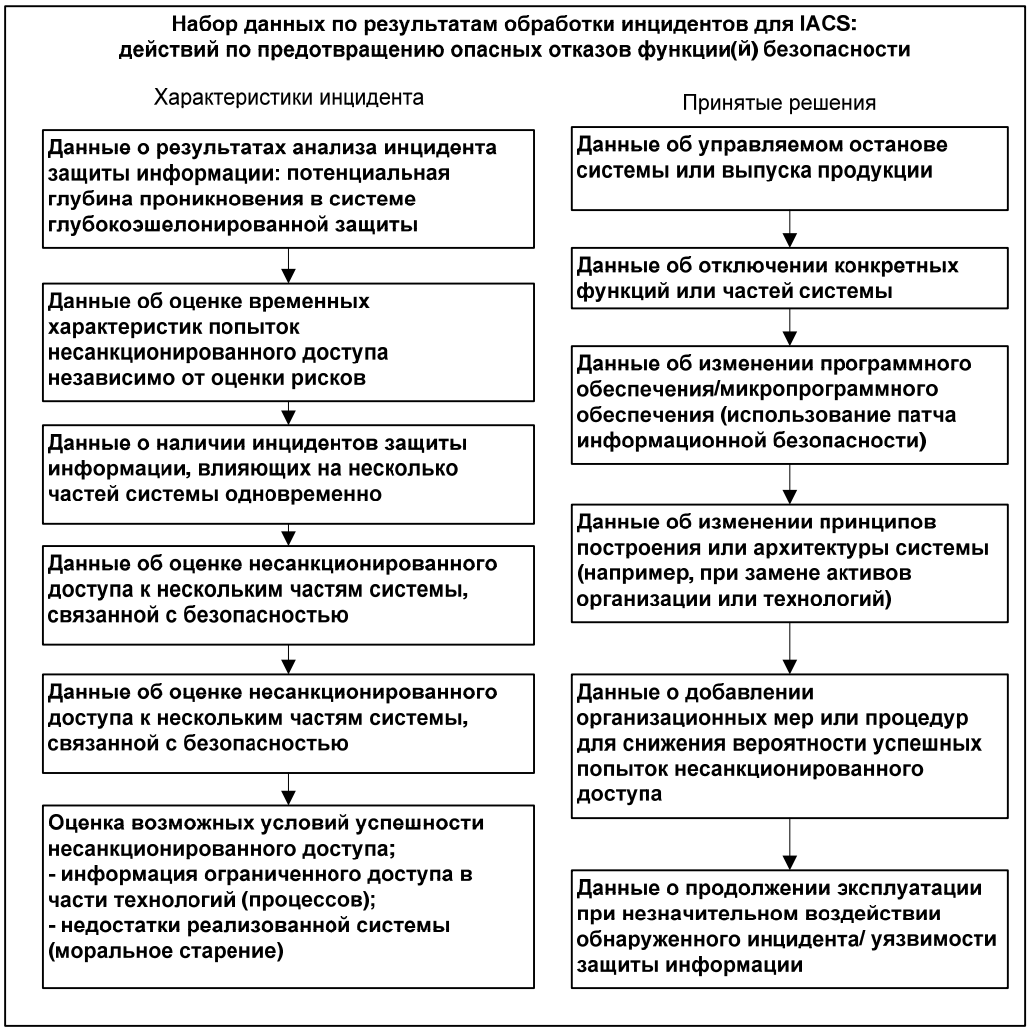

Рис. 19. **Набор данных IACS (вариант)**

При положительном решении организационных вопросов удаленного доступа надзорного органа к данным мониторинга подсистем ИБ и ФБ ОПО может быть обеспечено существенное сокращение продолжительности процедур сбора и обработки данных об инцидентах защиты информации. Существующие прецеденты системотехнических решений имеются, сведения о которых представлены в табл. 3.

Таблица 3

Характеристики систем удаленного мониторинга ИБ

Наименование решения	Перечень характеристик		
	сервисы	разработчик	рег. номер
База данных системы дистанционного контроля промышленной безопасности ОПО ООО «Газпром добыча Астрахань»	Текущие данные и архивная накопительная информация об ОПО. Сведения о проверках и выявленных несоответствиях. Справочники матриц опасных событий и регламентных значений параметров	ООО «Газпром добыча Астрахань»	2021621741 от 16 авг. 2021 г.
Система управления промышленной безопасностью «Безопасное предприятие»	Автоматизированный контроль за безопасностью на ОПО. Систематизация документооборота идентификация, анализ и прогнозирование риска аварий и связанных с авариями угроз. Координация по разработке и реализации мер по снижению риска аварий	ООО НПО «Диагностика и анализ риска»	2014615407 от 27 мая 2014 г.

В период с 1 февраля 2021 г. по 31 декабря 2023 г. в соответствии с постановлением Правительства Российской Федерации[27] проводилась апробация применения на ОПО системы дистанционного контроля пожарной безопасности под эгидой Ростехнадзора. Планировалось подключение систем контроля параметров оборудования, аварийных остановок, противопожарной защиты, оповещения, локации работников. Однако кардинальных изменений в цифровую трансформацию надзорной деятельности в форме дистанционного объективного (инструментального) контроля в режиме онлайн по ряду объективных причин, в том числе актуализации владельцами ОПО данных об активах, вытекающей из этого проблематичности реализации предиктивного анализа, не привнесла[28]. Поэтому было принято решение о переносе срока окончания мероприятий до 31 декабря 2025 г.[29] Вместе с тем ряд отечественных компаний создает и внедряет корпоративные системы дистанционного контроля пожарной безопасности, в частности, аналогичная система ПАО «Газпром автоматизация» в 2020 г. распространена на фонд скважин Астраханского Газоконденсатного месторождения, систему промысловых трубопроводов и газоконденсатопроводов, шесть установок предварительной подготовки газа и парк резервуарный (промысловый)[30]. Теоретическая проработка технологий реализации систем дистанционного контроля пожарной безопасности, в настоящее время продолжается различными исследовательскими коллективами [14–16].

[27] О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности: постановление Правительства Рос. Федерации (вместе с положением «О проведении эксперимента по внедрению системы дистанционного контроля промышленной безопасности») от 31 дек. 2020 г. № 2415. Доступ из справ.-правового портала «Гарант».

[28] Харас Б. Проблемы дистанционного мониторинга, контроля и надзора за эксплуатацией объектов ТЭК и промышленности // Информационно-аналитический журнал «Рубеж». 2023. 8 сент.

[29] О внесении изменения в постановление Правительства Рос. Федерации от 31 дек. 2020 г. № 2415: постановление Правительства Рос. Федерации от 9 дек. 2023 г. № 2099. Доступ из справ.-правового портала «Гарант».

[30] Gazprom-auto. URL: https://www.gazprom-auto.ru/press/news/884720/ (дата обращения: 23.08.2024).

– Выявление аномалий в данных об инцидентах защиты информации, соотнесение выявленных аномалий с локацией (предприятие, цех, участок, площадка) и пространственным (площадным) размещением, прогноз темпов развития аномалий на основе исторического профилирования и статистического анализа по подсистемам и функциям обеспечения безопасности конкретного ОПО. Исследование технологий обнаружения и выявления аномалий в процессе функционирования роботизированных систем с целью поддержания требуемых показателей безопасности представлено в работе [17].

– Прогнозная оценка потенциального ущерба с учетом темпов развития выявленных аномалий на конкретном ОПО [18].

– Оценка и принятие решения о целесообразности проведения профилактических мероприятий непосредственно на ОПО в требуемой точке локации (предприятие, цех, участок, площадка) с учетом удаленности объекта (пространственного размещения), допустимого резерва времени и ресурса специалистов государственного пожарного надзора.

– Проведение целевых профилактических мероприятий непосредственно на ОПО в требуемой точке локации.

– Анализ данных выявленных аномалий с целью определения изменений значений показателей соответствующих характеристик по подсистемам и функциям обеспечения безопасности конкретного ОПО по результатам профилактических мероприятий и принятие решения по завершению или продолжению проведения мероприятий по выявленной аномалии.

Процедуры организации профилактических мероприятий государственного пожарного надзора в соответствии с положениями методологии обеспечения ИБ и защиты информации на опасном производственном объекте, с учетом ФБ и пожарной безопасности объекта, представлены на рис. 20.

Процедуры выявления аномалий в данных об инцидентах ИБ базируются на моделях и методах оценки защищенности информации и ИБ технологических процессов с применением модели связности ИБ, ФБ и пожарной безопасности ОПО и оригинальных операций над матрицами связности данных с целью минимизации временных и ресурсных затрат при реализации процедур в прикладных системах.

Процедуры принятия решений о целесообразности проведения профилактических мероприятий территориальным органом государственного пожарного надзора с целью предотвращения инцидентов промышленной безопасности базируются на типовых и уточненных методах, моделях и средствах выявления, идентификации, классификации и анализа угроз нарушения ИБ непосредственно на ОПО.

Рис. 20. **Процедуры организации профилактических мероприятий государственного пожарного надзора**

Выводы

Бурный рост цифровых технологий, темпы цифровой трансформации различных сфер деятельности человека и общества, наукоемкость формирования современных международных требований и их гармонизация национальными регуляторами в области ИБ, ФБ и пожарной безопасности ОПО находятся в объективном противоречии с темпами технологического перехода на комплексные технологии обеспечения промышленной безопасности и внедрением передовых технологических решений в практику предприятий и отраслей экономики.

Достаточно актуальным и значимым является коллаборация ученых и специалистов различных отраслей знаний и предметной области для конструктивного разрешения текущих проблем обеспечения промышленной безопасности ОПО. Учитывая переход экономических укладов к экономике данных и цифровой трансформации государства, приоритетной задачей является обеспечение ИБ с учетом обеспечения ФБ технологических процессов и производств.

Затронутые в статье проблемы представляют собой методологическую основу структурированной парадигмы проактивной государственной пожарной надзорной деятельности, в рамках установленных правовыми актами полномочий и возможностей, основанной на моделях и методах оценки защищенности информации и ИБ технологических процессов и модели связности ИБ, ФБ и пожарной безопасности ОПО.

Как показали результаты исследования дальнейшие усилия целесообразно сосредоточить на реализацию способов оперативной оценки и реагирования на комплексные риски с учетом компромиссных решений в области ИБ.

Статья подготовлена в рамках выполнения НИР «Киберсреда» по государственному заданию МЧС России на 2024 г.

Список источников

1. Лившиц И.И., Сунцова Д.И. Численный расчет функциональной безопасности компонент технически сложных промышленных объектов // Автоматизация промышленности. 2023. № 8. С. 9–15.

2. Индык Ю.Д., Можаева И.А., Струков А.В. Выбор и обоснование компонентов ПАЗ с учетом требований полноты безопасности подтверждение соответствия // Актуальные проблемы защиты и безопасности: труды XXVI Всерос. науч.-практ. конф. СПб., 2023. С. 245–253.

3. Можаева И.А., Струков А.В. Особенности оценки показателей функциональной безопасности систем противоаварийной автоматической защиты с использованием деревьев неисправностей // Надежность. 2022. Т. 22. № 4. С. 45–52.

4. Струков А.В., Можаева И.А. Приближенные и упрощенные методы расчета показателей функциональной безопасности систем противоаварийной автоматической защиты // Актуальные проблемы защиты и безопасности: труды XXVII Всерос. науч.-практ. конф. СПб., 2024. С. 550–557.

5. Нозик А.А., Можаева И.А., Струков А.В. Методы решения прямой и обратной задачи оценки функциональной безопасности систем противоаварийной автоматической защиты // Актуальные проблемы защиты и безопасности: труды XXIII Всерос. науч.-практ. конф. Рос. акад. ракетных и артиллерийских наук (РАРАН). М., 2020. С. 196–211.

6. Можаева И.А., Нозик А.А., Струков А.В. Типовые примеры расчета функциональной безопасности систем противоаварийной защиты опасных производственных объектов // Актуальные проблемы защиты и безопасности: труды XXII Всерос. науч.-практ. конф. РАРАН. 2019. С. 486–494.

7. Бочков К.А., Буй П.М., Комнатный Д.В. Гармонизация требований по информационной безопасности различных объектов защиты // Комплексная защита

информации: материалы XXVI Науч.-практ. конф. / отв. за вып. С.Н. Касанин. Гомель, 2021. С. 220–226.

8. Wenze X., Jianghong J. Summary of Integrated Application of Functional Safety and Information Security in Industry: 12th International Conference on Reliability, Maintainability, and Safety (ICRMS). 2018. P. 463–469. DOI: 10.1109/ICRMS.2018.00092.

9. Sliwinski M., Piesik E., Piesik J. Integrated functional safety and cyber security analysis / IFAC PapersOnLine 51-24 (2018). P. 1263–1270.

10. Systems engineering approach to functional safety and cyber security of industrial critical installations. In Safety and Reliability of Systems and Processes; Eds. / K.T. Kosmowski [et al.]. Gdynia Maritime University: Gdynia, Poland, 2020. P. 135–151.

11. Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management / K.T. Kosmowski [et al.] // Energies 2022. 15. 3610. P. 1–21. DOI: 10.3390/en15103610.

12. Карманов А.В., Орлова К.П. Метод определения показателей безопасности на критически важных объектах нефтегазовой отрасли // Губкинский университет в решении вопросов нефтегазовой отрасли России: тезисы докладов VI Рег. Науч.-техн. конф., посвящ. 100-летию М.М. Ивановой. М., 2022. С. 775–776.

13. Карманов А.В., Орлова К.П. Метод расчета показателей системы безопасности в составе АСУТП нефтегазовой отрасли // Губкинский университет в экосистеме современного образования: тезисы докладов V Рег. науч.-техн. конф. / отв. ред. В.Г. Мартынов. М., 2021. С. 44.

14. Перспективы развития дистанционного контроля промышленной безопасности в части контроля технологических параметров / Д.В. Ибадулаев [и др.] // Актуальные проблемы защиты и безопасности: труды XXVII Всерос. науч.-практ. конф. СПб., 2024. С. 483–495.

15. Ибадулаев Д.В., Степанов И.В., Турусов С.Н. Технологи создания алгоритмического обеспечения объектовой системы дистанционного контроля промышленной безопасности // Актуальные проблемы защиты и безопасности: труды XXVII Всерос. науч.-практ. конф. СПб., 2024. С. 522–527.

16. Опыт внедрения системы дистанционного контроля промышленной безопасности в части контроля технологических параметров / Д.В. Ибадулаев [и др.] // Актуальные проблемы защиты и безопасности: труды XXVI Всерос. науч.-практ. конф. СПб., 2023. С. 235–244.

17. Kirca Y.S., Değirmenci E., Demirci Z. and ets. Runtime Verification for Anomaly Detection of Robotic Systems Security // Machines. 2023. 11(2):166. DOI: 10.3390/machines11020166.

18. Матвеев А.В. Организационные и методические аспекты обеспечения безопасности потенциально опасных объектов. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2019. 144 с. ISBN 978-5-4268-0051-9. EDN JGVNSE.

References

1. Livshic I.I., Suncova D.I. Chislennyj raschet funkcional'noj bezopasnosti komponent tekhnicheski slozhnyh promyshlennyh ob"ektov // Avtomatizaciya promyshlennosti. 2023. № 8. S. 9–15.

2. Indyk Yu.D., Mozhaeva I.A., Strukov A.V. Vybor i obosnovanie komponentov PAZ s uchetom trebovanij polnoty bezopasnosti podtverzhdenie sootvetstviya // Aktual'nye problemy zashchity i bezopasnosti: trudy XXVI Vseros. nauch.-prakt. konf. SPb., 2023. S. 245–253.

3. Mozhaeva I.A., Strukov A.V. Osobennosti ocenki pokazatelej funkcional'noj bezopasnosti sistem protivoavarijnoj avtomaticheskoj zashchity s ispol'zovaniem derev'ev neispravnostej // Nadezhnost'. 2022. T. 22. № 4. S. 45–52.

4. Strukov A.V., Mozhaeva I.A. Priblizhennye i uproshchennye metody rascheta pokazatelej funkcional'noj bezopasnosti sistem protivoavarijnoj avtomaticheskoj zashchity // Aktual'nye

problemy zashchity i bezopasnosti: trudy XXVII Vseros. nauch.-prakt. konf. SPb., 2024. S. 550–557.

5. Nozik A.A., Mozhaeva I.A., Strukov A.V. Metody resheniya pryamoj i obratnoj zadachi ocenki funkcional'noj bezopasnosti sistem protivoavarijnoj avtomaticheskoj zashchity // Aktual'nye problemy zashchity i bezopasnosti: trudy XXIII Vseros. nauch.-prakt. konf. Ros. akad. raketnyh i artillerijskih nauk (RARAN). M., 2020. S. 196–211.

6. Mozhaeva I.A., Nozik A.A., Strukov A.V. Tipovye primery rascheta funkcional'noj bezopasnosti sistem protivoavarijnoj zashchity opasnyh proizvodstvennyh ob"ektov // Aktual'nye problemy zashchity i bezopasnosti: trudy XXII Vseros. nauch.-prakt. konf. RARAN. 2019. S. 486–494.

7. Bochkov K.A., Buj P.M., Komnatnyj D.V. Garmonizaciya trebovanij po informacionnoj bezopasnosti razlichnyh ob"ektov zashchity // Kompleksnaya zashchita informacii: materialy XXVI Nauch.-prakt. konf. / otv. za vyp. S.N. Kasanin. Gomel', 2021. S. 220–226.

8. Wenze X., Jianghong J. Summary of Integrated Application of Functional Safety and Information Security in Industry: 12th International Conference on Reliability, Maintainability, and Safety (ICRMS). 2018. P. 463–469. DOI:10.1109/ICRMS.2018.00092.

9. Sliwinski M., Piesik E., Piesik J. Integrated functional safety and cyber security analysis / IFAC PapersOnLine 51-24 (2018). P. 1263–1270.

10. Systems engineering approach to functional safety and cyber security of industrial critical installations. In Safety and Reliability of Systems and Processes; Eds. / K.T. Kosmowski [et al.]. Gdynia Maritime University: Gdynia, Poland, 2020. P. 135–151.

11. Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management / K.T. Kosmowski [et al.] // Energies 2022. 15. 3610. P. 1–21. DOI: 10.3390/en15103610.

12. Karmanov A.V., Orlova K.P. Metod opredeleniya pokazatelej bezopasnosti na kriticheski vazhnyh ob"ektah neftegazovoj otrasli // Gubkinskij universitet v reshenii voprosov neftegazovoj otrasli Rossii: tezisy dokladov VI Reg. Nauch.-tekhn. konf., posvyashch. 100-letiyu M.M. Ivanovoj. M., 2022. S. 775–776.

13. Karmanov A.V., Orlova K.P. Metod rascheta pokazatelej sistemy bezopasnosti v sostave ASUTP neftegazovoj otrasli // Gubkinskij universitet v ekosisteme sovremennogo obrazovaniya: tezisy dokladov V Reg. nauch.-tekhn. konf. / otv. red. V.G. Martynov. M., 2021. S. 44.

14. Perspektivy razvitiya distancionnogo kontrolya promyshlennoj bezopasnosti v chasti kontrolya tekhnologicheskih parametrov / D.V. Ibadulaev [i dr.] // Aktual'nye problemy zashchity i bezopasnosti: trudy XXVII Vseros. nauch.-prakt. konf. SPb., 2024. S. 483–495.

15. Ibadulaev D.V., Stepanov I.V., Turusov S.N. Tekhnologi sozdaniya algoritmicheskogo obespecheniya ob"ektovoj sistemy distancionnogo kontrolya promyshlennoj bezopasnosti // Aktual'nye problemy zashchity i bezopasnosti: trudy XXVII Vseros. nauch.-prakt. konf. SPb., 2024. S. 522–527.

16. Opyt vnedreniya sistemy distancionnogo kontrolya promyshlennoj bezopasnosti v chasti kontrolya tekhnologicheskih parametrov / D.V. Ibadulaev [i dr.] // Aktual'nye problemy zashchity i bezopasnosti: Trudy XXVI Vseros. nauch.-prakt. konf. SPb., 2023. S. 235–244.

17. Kirca Y.S., Değirmenci E., Demirci Z. and ets. Runtime Verification for Anomaly Detection of Robotic Systems Security // Machines. 2023. 11(2):166. DOI: 10.3390/machines11020166.

18. Matveev A.V. Organizacionnye i metodicheskie aspekty obespecheniya bezopasnosti potencial'no opasnyh ob"ektov. SPb.: S.-Peterb. un-t GPS MCHS Rossii, 2019. 144 s. ISBN 978-5-4268-0051-9. EDN JGVNSE.

Информация о статье:
Статья поступила в редакцию: 13.07.2024; одобрена после рецензирования: 21.09.2024; принята к публикации: 26.09.2024
Information about the article:
The article was submitted to the editorial office: 13.07.2024; approved after review: 21.09.2024; accepted for publication: 26.09.2024

Сведения об авторах:
Тукмачева Марина Алексеевна, адъюнкт Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), e-mail: mtukmacheva@mail.ru, https://orcid.org/0009-0004-2496-7117, SPIN-код: 2489-5760
Шестаков Александр Викторович, старший научный сотрудник, помощник начальника Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, e-mail: alexandr.shestakov01@yandex.ru, https://orcid.org/0000-0002-8462-6515, SPIN-код: 5831-5451

Information about the authors:
Tukmacheva Marina A., adjunct of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), e-mail: mtukmacheva@mail.ru, https://orcid.org/0009-0004-2496-7117, SPIN: 2489-5760
Shestakov Alexander V., senior researcher, assistant chief of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of engineering sciences, e-mail: alexandr.shestakov01@yandex.ru, https://orcid.org/0000-0002-0778-32180000-0002-8462-6515, SPIN: 5831-5451