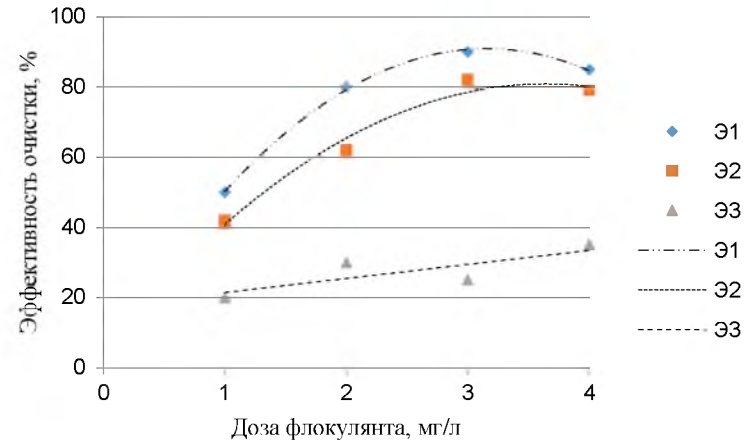


Рисунок 2 – Зависимость эффективности очистки от дозы флокулянта:
Э1 – Praestol 853, Э2 – Praestol 852, Э3 – Praestol 2540

**Заключение**

В результате проведенных экспериментальных исследований было установлено, что наиболее высокую очистку льяльных вод от средне- и грубодисперсных нефтяных частиц обеспечивает ионногенный флокулянт Praestol 853. Так, использование флокулянта Praestol 853 в качестве реагента при флотационной очистке судовых льяльных вод при дозе 3 мг/л позволяет извлечь более 90 % нефтяных загрязнений.

**Литература**

1. Тихомиров Г.И. Анализ методов и технических средств очистки льяльных вод / Г.И. Тихомиров // Транспортное дело России. – 2015. – № 6 – С. 288-292.
2. Гетманцев С.В. Очистка производственных сточных вод коагулянтами и флокулянтами / С.В. Гетманцев, И.А. Нечаев, Л.В. Гандурина. – М.: АСВ, 2008.
3. Пономарев В.Г. Образование и очистка сточных вод нефтеперерабатывающих заводов / В.Г. Пономарев, Э.Г. Иоакимис. – М.: Союз Дизайн, 2009.
4. Вейцер Ю.И. Высокомолекулярные флокулянты в процессах очистки воды.– М.: АСВ, 2010.
5. Технический справочник по проблемам воды / К. Барак, Ж. Бебен, Ж. Бернар и др. –М.: АСВ, 2007.
6. Епихин А.И., Кондратьев С.И., Хекерт Е.В. Применение нейронных сетей на базе многослойного перцептрона с использованием нечеткой логики для технической диагностики судовых технических средств// Эксплуатация морского транспорта.– 2020.– № 3 (96).– С. 111-119.

***References***

1. Tikhomirov G I 2015 Analysis of methods and technical means of bilge water treatment Transportation in Russia. – № 6 – pp 288–292.
2. Getmantsev S.V. Ochistka promishlennih stochnih vod koagulyantami i flokulyantami Moscow, ASV, 2008
3. Ponomaryov V.G. Obrazovanie i ochistka stochnih vod neftepererabativayushih zavodov, Moscow, Soyuz-Dizayn, 2009
4. Veytser Yu.I. Visokomolekulyarnie flokulyanti v protsessah ochistki vodi, Moscow, ASV, 2010
5. Tehnicyeskiy spravochnik po problemam vodi, Moscow, ASV, 2007.
6. Epikhin A.I., Kondratiev S.I., Hekert E.V. Application of neural networks based on a multilayer perceptron using fuzzy logic for the technical diagnosis of ship technical means// Operation of sea transport. 2020. No. 3 (96). pp. 111-119.

**УДК 629**
DOI: 10.34046/aumsuomt101/27

# УЧЁТ КИБЕРРИСКОВ ПРИ УПРАВЛЕНИИ БЕЗОПАСНОСТЬЮ ЭКСПЛУАТАЦИИ ЭНЕРГЕТИЧЕСКОГО ОБОРУДОВАНИЯ ПЛАВУЧЕЙ РЕГАЗИФИКАЦИОННОЙ УСТАНОВКИ

*В. А. Туркин, доктор технических наук, профессор*
*Д. А. Давыдов, аспирант*
*А. А. Стяжкин, аспирант*

Требования резолюций Международной морской организации (ИМО) предусматривают необходимость организовать управление киберрисками в системах управления безопасностью судоходства. В

статье в качестве критерия оценки уровня и обеспечения безопасности представлен техногенный риск, под которым понимается мера возможных опасностей, одновременно учитывающая частоту возникновения нежелательного события и последствия реализации нежелательного события. Представлены результаты анализа эксплуатации плавучих регазификационных установок сжиженного природного газа, основанные на опыте эксплуатации и собранных статистических данных. Построена модель «дерево отказов» результирующим событием в которой является утечка газа. Установлено, что «утечка газа» может произойти с частотой 0.4 1/год. Рассмотрены подсистемы управления судоходной компании, которые позволяют осуществлять дистанционный контроль и управление энергетическими установками и оборудованием. Недостатком систем является их уязвимость для кибератак. На основании анализа публикаций классификационного общества DNV было выявлено восемь основных уязвимостей в области кибербезопасности плавучей регазификационной установки. Исходя из статистики кибератак на инфраструктуру промышленных предприятий РФ в 2019 г. установлено, что частота кибератак на судовые технические средства примерно составит 0.009 1/год.

**Ключевые слова:** Плавучая регазификационная установка, энергетическое оборудование, безопасность, цифровизация, оценка риска, частота кибератак

# ACCOUNTING FOR CYBER RISKS IN THE SAFETY MANAGEMENT OF THE OPERATION OF POWER EQUIPMENT OF A FLOATING REGASIFICATION PLANT

*V. A. Turkin, D. A. Davydov, A. A. Styazhkin*

The requirements of the resolutions of the International Maritime Organization (IMO) provide for the need to organize the management of cyber risks in navigation safety management systems. The article presents technogenic risk as a criterion for assessing the level and ensuring safety, which is understood as a measure of possible hazards, simultaneously taking into account the frequency of occurrence of an undesirable event and the consequences of the implementation of an undesirable event. The results of the analysis of the operation of floating regasification units of liquefied natural gas, based on operational experience and collected statistical data, are presented. The model "tree of failures" is constructed, the resulting event in which is a gas leak. It is established that a "gas leak" can occur with a frequency of 0.4 1/year. The management subsystems of a shipping company that allow remote control and management of power plants and equipment are considered. The disadvantage of the systems is their vulnerability to cyber attacks. Based on the analysis of publications of the DNV classification society, eight main vulnerabilities in the field of cybersecurity of a floating regasification installation were identified. Based on the statistics of cyberattacks on the infrastructure of industrial enterprises of the Russian Federation in 2019, it was found that the frequency of cyberattacks on ship equipment will be approximately 0.009 1/year.

**Keywords**: Floating regasification plant, power equipment, security, digitalization, risk assessment, frequency of cyber attacks.

## Введение

Стремительное распространение информационных технологий и их проникновение во все сферы человеческой деятельности привело к созданию принципиально новых систем управления техническими и организационными объектами в промышленности и на транспорте [1]. Увеличивающаяся интенсивность судоходства, возрастающие объемы перевозок опасных грузов повышают и риск возникновения аварийных ситуаций, и масштабы возможного ущерба.

Современной общемировой тенденцией стала прогрессирующая цифровизация экономики, что в полной мере касается морского и речного транспорта. Вследствие всё большей автоматизации технологических процессов численность судовых экипажей уменьшается. Некоторые бортовые системы получают обновления во время плавания, у команд есть выход в Интернет. По мнению ряда специалистов, вопросам информационной безопасности объектов морской и речной транспортной инфраструктуры, морских и речных судов уделяется мало внимания. Как правило, в описании услуг, продуктов и решений вопросы информационной безопасности не затрагиваются.

В контексте рассматриваемой проблематики под информационной безопасностью судовой информационной системы понимается защищенность информации на судне и поддерживающей её инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Соответственно, под защитой информации на судне понимается комплекс мероприятий, направленных на обеспечение информационной безопасности судовой информационной системы и включающих, в первую очередь, мероприятия по защите от атак, искажений информации, внешних воздействий и несанкционированного доступа к каналам передачи данных. Главная задача судовой информационной системы заключается в информационном содействии намерениям: судоводителя – в обеспечении его актуаль-

ными, убедительными и достоверными динамическими (навигационными), рейсовыми и текстовыми сведениями, касающимися безопасности плавания и необходимыми для принятия решений управления судном [1, 2, 3]; судомеханика – в управлении главной энергетической установкой, электростанцией, механизмами и системами машинного отделения и контроля параметров [4,5].

Постановка проблемы

Международной морской организацией 16 июня 2017 года была принята резолюция MSC.428(98) «Управление киберрисками в морской отрасли в рамках систем управления безопасностью» [6], а также выпущен циркуляр MSC-FAL.1/Circ.3 «Руководство по управлению киберрисками в морской отрасли» [7]. Резолюция [6] предусматривает необходимость в повышении осведомленности персонала судоходных компаний и членов экипажа относительно угроз киберрисков для поддержания безопасного и защищенного судоходства. Российский морской регистр судоходства (РМРС – RS) также подготовил «Руководство по обеспечению кибербезопасности» [8], действующее с 1 января 2021 года.

В соответствии требованиям Резолюции ИМО [6] и Руководства RS [8] в утвержденной Системе управления безопасностью (СУБ) судоходной компании должно учитываться управление киберрисками в соответствии с целями и функциональными требованиями Международного кодекса по управлению безопасной эксплуатацией судов и предотвращением загрязнения (МКУБ) [9]. Киберриски должны быть учтены в СУБ не позднее, чем во время первой ежегодной проверки Документа о соответствии компании после 01 января 2021 года.

В Руководстве RS указано, что специфические требования, связанные с управлением киберрисками, каждая компания может вносить в существующую СУБ. Эти вопросы компания определяет самостоятельно. Указано, что такая интеграция в СУБ должна соответствовать резолюции ИМО MSC.428(98) [6] и циркуляру ИМО MSC-FAL.1/Circ.3 [7].

Дополнительно Руководство RS указывает, какие разделы должны быть включены в соответствующую интегрированную процедуру СУБ: цели и политика, оценка риска, ресурсы и персонал, отчеты и т. п. Руководство RS содержит рекомендации по проектированию, изготовлению, обслуживанию и проведению испытаний судовых компьютеризированных систем, а также определяет рекомендации, применимые к системам управления безопасностью (СУБ). Рекомендации Руководства направлены на реализацию положений резолюции ИМО MSC.428(98), в соответствии с которыми, не позднее, чем во время первой ежегодной проверки Документа о соответствии компании (ДСК), после 01 января 2021 года необходимо учитывать киберриски в СУБ согласно положениям циркуляра ИМО MSC-FAL.1/Circ.3 [7].

Оценка параметров риска эксплуатации грузового оборудования плавучей регазификационной установки

На основании анализа различных определений и с учетом сложившейся в последнее время в сфере управления техногенной безопасностью практики [10, 11] величина риска может быть рассчитана как произведение частоты нежелательного события на ущерб, вызванный этим событием. Математически данное определение может быть записано в виде следующего выражения:

$$R_A = \lambda_A \cdot Y, \qquad (1)$$

где $R_A$ – величина риска аварии (год$^{-1}$) или (руб. год$^{-1}$); $\lambda_A$ – частота реализации аварии рассматриваемого типа (год$^{-1}$); $Y$ – ущерб от аварии (без размерности или руб).

Размерность (год$^{-1}$) используется в том случае, если оценивается риск гибели человека (индивидуальный риск), а размерность (руб. год$^{-1}$) – если оценивается риск потери материальных ценностей или экологический риск.

Основная цель регазификационной установки, схема которой показана на рисунке 1, – испарение сжиженного природного газа (СПГ) с последующей его подачей в береговой трубопровод. На вход в установку СПГ из грузовых танков судна подаётся питательными регазификационными насосами при давлении около 5,5 бар и температуре (-160) °С. На выходе из установки газ уже находится под давлением 60-80 бар при температуре 0°С [12].

Анализ эксплуатации плавучей регазификационной установки (ПРГУ) показывает, что с точки зрения опасности высвобождения СПГ в газообразной форме в атмосферу, значение имеет процесс его регазификации. Во время анализа стоит учитывать, что во время работы ПРГУ в стационарном режиме регазификации, риски эксплуатации должны быть частично пересмотрены и обновлены в силу особенностей эксплуатации судна и его устройств. С этой точки зрения, анализ рисков ПРГУ как танкера-газовоза становится менее точным и целесообразнее рассматривать его уже как плавучий терминал СПГ.

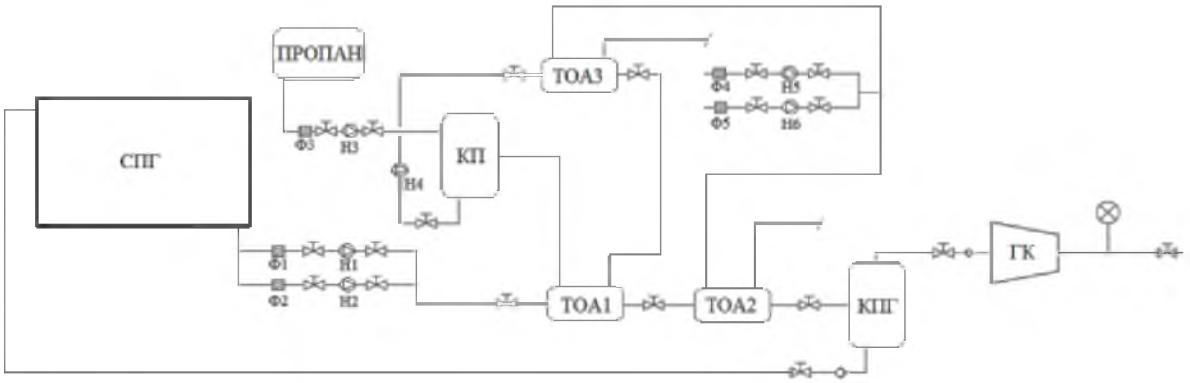


Рисунок 1 – Принципиальная схема двухступенчатой ПРГУ: СПГ – танк со сжиженным природным газом; Пропан – танк со сжиженным пропаном; КП – конденсатор пропана; ТОА 1, 2, 3 – теплообменные аппараты: № 1 – пропан – СПГ; № 2 – пропан – забортная вода; № 3 – природный газ – забортная вода; КПГ – конденсатор природного газа; ГК – грузовой компрессор; Н1, Н2 – питательные регазификационные насосы; Н3, Н4 – насосы подачи пропана; Н5, Н6 – насосы забортной воды; Ф1, 2, 3, 4, 5 – фильтры: № 1, 2 – сжиженного природного газа; № 3 – пропана; № 4, 5 – забортной воды

Результаты собранной статистической информации показали, что одними из основных причин, приводящих к нарушению работы ПРГУ, являются отказы в работе клапанов, нарушения в работе операционных систем по управлению оборудованием установки, а также, подконтрольных им, исполнительных механизмов, неисправности аварийно-предупредительных систем, повреждения и эксплуатационный износ трубопроводов.

Так, анализ статистики аварий результирующих в выброс природного газа в атмосферу за 2019 год показал, что на 135 терминалах, 41 авария произошла в результате нарушения работы управляющих / предохранительных клапанов, из которых 11 случаев произошли в результате нарушения работы или непреднамеренного срабатывания аварийной системы прекращения подачи груза (Emergency shutdown system – ESDS). Основными причинами стали: срабатывание ESD-клапана, раньше установленного предельно допустимого давления, непроизвольное срабатывание или же несрабатывание автоматической системы управления ESD-клапаном, зависание ESD-клапана в промежуточном состоянии по механическим причинам.

Общий финансовый ущерб от произошедших аварий составил 20.3 млн. долларов. За исключением единичной аварии, ущерб от которой составил 18 млн. долларов, доля ущерба на оставшиеся инциденты составляет порядка 2.3 млн. долларов. Цена ущерба включает в себя: цену потерянного количества газа и простой, ущерб собственности терминала, ущерб персоналу терминала, издержки за загрязнение окружающей среды, создание аварийной ситуации, а также затраты на проведение расследования. Помимо этого 21 авария связана с компрессорным отделением подачи газа, из которых 6 аварий связаны с отказом грузового компрессора и 15 аварий связаны с оборудованием компрессорного отделения, отказ которого, стал начальным этапом аварий, повлекших за собой утечку газа. Общий финансовый ущерб от произошедших аварий составил более 1.6 млн. долларов.

Опираясь на статистику, можно отметить, что основная часть аварий, а именно – 56, произошла в результате разрушения или повреждения газопровода. Из них 46 произошло в результате разного рода износа трубопровода старше 25 лет, и только 10 аварий пришлись на фланцевые соединения, сварочные швы и трубопроводы, сроком эксплуатации менее 10 лет.

Основываясь на результатах анализа собранной статистической информации и материалов научных исследований, приведенных литературных источниках [12, 13, 14, 15], построена показанная на рисунке 2 модель «дерево отказов».

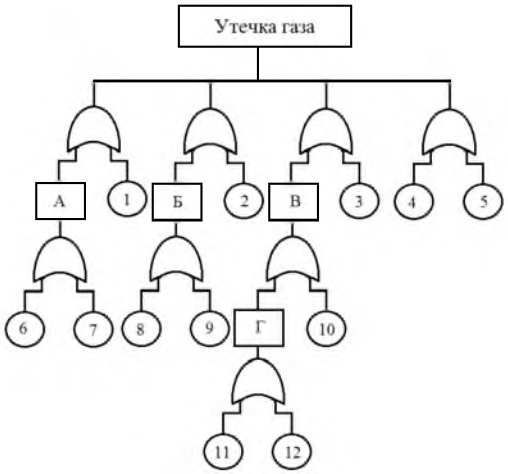


Рисунок 2 – Модель «дерево отказов» для режима регазификации

Целью модели является определить величину риска отказа оборудования и механизмов, взаимодействующих с ПГ в жидкой, газообразной и частично газообразной форме.

Анализ рисков эксплуатации установки производился исходя из того факта, что часть её оборудования взаимодействует с СПГ в жидкой фазе, а часть в газообразной.

Стоит отметить, что в построенной модели «дерево отказов» результирующим событием является утечка газа и, соответственно, во время анализа рисков, из статистки вычленялись, рассматривались и учитывались отказы, которые приводили к данному событию.

В таблице 1 приведены значения частот возникновения нежелательных событий, показанных на рисунке 2. Анализ таблицы 1 показывает, что результирующее нежелательное событие «Утечка газа» может происходить с частотой 0.4 (год$^{-1}$), то есть один раз в 2.5 года. Учитывая, что при совмещении данного нежелательного события с наличием открытого источника воспламенения может произойти взрыв парогазовой смеси, следует сделать вывод о необходимости принятия мер для снижения частоты возникновения события «Утечка газа».

Таблица 1 – Описание цифровых обозначений, приведенных на рисунке 2, и значения частот возникновения нежелательных событий

| Событие | Частота события (год$^{-1}$) |
|---|---|
| 1. Несрабатывание главного клапана прекращения подачи газа при подаче на него сигнала закрытия (ESD) | 0.081481 |
| 2. Разрушение трубопровода сроком службы более 25 лет | 0.340740 |
| 3. Отказ оборудования компрессорного отделения, являющийся начальным этапом аварии, повлекших за собой утечку газа | 0.01111 |
| 4. Отказ предохранительного / регулирующего оборудования | 0.055555 |
| 5. Отказ привода предохранительного / регулирующего оборудования | 0.055555 |
| 6. Непреднамеренное срабатывание автоматической системы аварийного прекращения подачи газа ESDS, влекущее за собой закрытие главного клапана | 0.0296296 |
| 7. Нарушение в работе модулей мониторинга автоматической системы аварийного прекращения подачи газа ESDS | 0.0074074 |
| 8. Износ или разрушение трубопровода сроком службы менее 10 лет | 0.037037 |
| 9. Утечка в результате неплотности фланцевого соединения или сварного шва | 0.02222 |
| 10. Отказ в работе грузового компрессора по техническим причинам | 0.007407 |
| 11. Отказ в работе грузового компрессора по причине неисправности модулей считывания состояния компрессора. | 0.007407 |
| 12. Отказ грузового компрессора по причине неисправности системы автоматического управления и мониторинга компрессора | 0.02962963 |
| А. Нарушение работы системы аварийного прекращения подачи газа (ESDS) | 0.037037 |
| Б. Утечка газа в результате неисправности газопровода. | 0.059257 |
| В. Утечка газа в результате нарушения работы грузового компрессора | 0.04363888 |
| Г. Отказ компрессора по причине неисправности автоматики | 0.03623188 |
| **Результирующее событие «Утечка газа»** | **0.4** |

Предложенный подход позволяет более углублённо и комплексно провести оценку риска эксплуатации ПРГУ, а так же заблаговременно выявить слабые узлы установки, в перспективе, приводящие к её отказу и требующие повышенного внимания.

В дерево отказов не были включены: аварии, расследование которых на данный момент не завершено, влияние человеческого фактора и тренированности персонала, влияние защищённости систем управления (кибербезопасности), а также отказ внутренних элементов систем автоматического управления.

Учёт киберрисков при эксплуатации судового энергетического оборудования

Внедрение цифровых технологий в энергетическую отрасль революционизирует процессы производства, хранения, транспортировки и потребления энергии. Эти разработки позволили значительно улучшить доступность и эффективность энергетических установок, упростить управление ими. Но они также открывают возможность кибератак.

До недавнего времени энергетическая отрасль практически не подвергалась риску кибератак, поскольку в основном использовалось механическое или аналоговое оборудование, а также запатентованные программы или протоколы, характерные для каждой операции или установки. Их можно было атаковать только с детальным знанием систем, в то время как отсутствие связи с внешним миром ограничивало возможности кибершпионажа [16, 19, 20, 21].

Впоследствии три фактора привели к постепенной интеграции информационных технологий (ИТ) в энергетическую отрасль: необходимость рационализации производства с помощью инструментов, способных собирать и обрабатывать большие объемы данных; необходимость обмениваться данными с субъектами за пределами промышленных площадок секторов; необходимость сэкономить на используемом программном обеспечении и облегчить взаимодействие между узлами управления.

Чтобы удовлетворить указанные потребности, энергетическая отрасль постепенно пришла к использованию операционных систем и промышленных систем управления (Industrialcontrolsystems – ICS). Промышленные системы управления – это информационные системы, используемые для управления и автоматизации многочисленных производственных процессов. Они широко используются в энергетике и, как известно, уязвимы для кибератак. Таким образом, системы управления судоходных компаний стали опираться на 4 подсистемы: операционных технологий (ОТ), информационных технологий (ИТ), промышленных систем управления (ПСУ) и систем диспетчерского управления и сбора данных (SCADA) [17,18,21].

Согласно данным компании Positive Technologies (https://www.ptsecurity.com/ru-ru/about/ ) за 2019 год было совершено 125 атак на инфраструктуру промышленных предприятий Российской Федерации, 110 были совершены с целью похищения данных компании, остальные 12 с целью получения финансовой выгоды. Если исходить из допущения, что финансовые убытки, понесённые компанией за счёт простоя судна или других остановок в производстве, принесут выгоду компании-оппоненту или третьим лицам, а сама ПРГУ является частью нефтегазовой промышленности, то можно рассчитать частоту осуществления кибератак. На данный момент в России насчитывается 1323 промышленных предприятия и производства. Исходя из этого можно примерно вычислить частоту кибератак на ПРГУ и судовые технические средства, она составит 0.00907029 (год$^{-1}$).

Уязвимости в области кибербезопасности можно устранить с помощью подхода, основанного на оценке риска. Это позволяет компаниям выявлять угрозы и уязвимости операций и планировать барьеры для предотвращения инцидентов и смягчения последствий. Для того чтобы установить эти барьеры и обеспечить безопасность систем управления и мониторинга работы ПРГУ, систем, устройств и судна следует: убедиться, что все передачи данных имеют проверки целостности; следить за блокировкой и защитой доменных имен; по возможности, сегментировать сеть управления, чтобы предотвратить распространение вредоносных программ после того, как целевая сеть или система были взломаны; применять двухфакторную аутентификацию; обучать и держать сотрудников в курсе текущих угроз, повышать их осведомленность в вопросах информационной безопасности.

Заключение

Новые требования резолюций IMO и нового руководства RS предусматривают необходимость организовать управление киберрисками в системах управления безопасностью не позднее первой ежегодной проверки Документа о соответствии компании после 1 января 2021 г.

В качестве критерия оценки уровня и обеспечения безопасности представлен техногенный риск, под которым понимается мера возможных опасностей, одновременно учитывающая частоту возникновения нежелательного события и его последствия.

На основании анализа статистической информации и материалов научных исследований построена модель «дерево отказов», целью которой является определить частоты отказов оборудования и механизмов, взаимодействующих с природным газом. Установлено, что результирующее нежелательное событие «Утечка газа» может произойти с частотой 0.4 (год$^{-1}$).

Рассмотрена архитектура системы управления судоходной компании, которая опирается на 4 подсистемы: операционных технологий, информационных технологий, промышленных систем управления и систем диспетчерского управления и сбора данных (SCADA). Недостатком систем является их уязвимость для кибератак.

Исходя из статистики кибератак на инфраструктуру промышленных предприятий РФ в 2019 г. установлено, что частота кибератак на судовые технические средства составит 0.009 (год$^{-1}$).

***References***

1. Zhestovskij A G, Mikhailovskij M Yu, Okolot D Ya, Rudinskij I D 2019 The problems of information security of shipboard information system and ways of their solution when training specialists of marine directions *Marine intellectual technologies* 4(46)-4 93-101
2. Boran-Keshishyan A L, Astrein V V, Kondratiev S I 2019 Formalization of the general strategy of decision making to achieve complex safety of the ship *Marine intellectual technologies* 1(43)-2.– 127-131

3. Astrein V V, Kondratiev S I, Boran-Keshishyan A L 2019 Presentation precedent in ship DSS of safe navigation *Marine intellectual technologies* 4(46)-**3** 147-152
4. Ivanchenko A A, Turkin V A, Karakayev A B, Konev G A 2019 State and perspective directions of development of CAD in shipbuilding *Marine intellectual technologies* 1(43)-2 41-45
5. Samoilenko A Yu, Turkin V A, Bushlanov V P 2019 The formation of the experimental database for the study of cycles marine diesel engines *Marine intellectual technologies* 1(43)-2 59-62
6. IMO 2017 Maritime Cyber Risk Management in Safety Management Systems. MSC.428(98) (London: IMO)
7. IMO 2017 Guidelines On Maritime Cyber Risk Management. MSC-FAL.1/Circ.3. (London: IMO)
8. RS 2021 Guidelines on Cyber Safety (ND No. 2-030101-040-E) (St. Petersburg: Russian Maritime Register of Shipping) 46
9. IMO 1993 The International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code), Resolution A.741(18) (London: IMO)
10. Reshnyak V I, Zakharov V N, Mizgiryov D S, Slyusarev A S 2019 The ecological risk assessment during accidental oil spills at water transport objects *Marine intellectual technologies* 4(46)-2 85-90
11. Reshnyak V I 2019 The theoretical basis assessment of risk emergency of oil spills *Marine intellectual technologies* 4(46)-3 72-76
12. Marcelo Ramos Martins and Adriana Miralles Schleder 2012 Reliability Analysis of the Regasification System on Board of a FSRU Using Bayesian Networks, Natural Gas - Extraction to End Use, Sreenath Borra Gupta, IntechOpen, DOI: 10.5772/45803
13. Pipeline and Hazardous Material Administration. https://www.phmsa.dot.gov/ (date of the application 16.03.2021)
14. Hidalgo E M P, Silva D W R and de Souza G F M 2013 Probabilistic corrosion failure analysis of a LNG carrier loading pipeline *22nd International Congress of Mechanical Engineering (COBEM 2013) November 3-7, 2013* (Ribeirão Preto, SP, Brazil) 3113-3123
15. Vianello C, Maschio G 2014 Risk analysis of lng terminal: case study *Chemical Engineering Transactions* 36 277-282 DOI: 10.3303/CET1436047
16. Desarnaud G 2017 Cyber Attacks and Energy Infrastructures: Anticipating Risks *Etudes de l'Ifri* (Paris: Ifri) 60
17. Protecting the connected barrels. Cybersecurity for upstream oil and gas. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/energy-resources/DUP_Protecting-the-connected-barrels.pdf (date of the application 16.03.2021)
18. Epikhin A.I. and Bashurov B P 2019 Experience and trends in the application of ship vehicles for LNG in vessels of the port fleet in the Russian Federation and the world *Marine intellectual technologies* 4(46)-3 52-58
19. Epikhin A.I., Kondratiev S.I., Hekert E.V. Application of neural networks based on a multilayer perceptron using fuzzy logic for technical diagnostics of ship technical means//Operation of sea transport. 2020. No. 3 (96). pp. 111-119.
20. Epikhin A.I., Kondratiev S.I., Hekert E.V.Prediction of multidimensional nonstationary time series using neuromodeling// Marine intelligent technologies. 2020. No. 4-4 (50). pp. 23-27.
21. Kondratiev S.I. Synthesis of program trajectories by the method of dynamic programming [Text] / S.I. Kondratiev // News of higher educational institutions. The North Caucasus region. Series: Technical Sciences. 2003.No. S6. pp. 41-43.


**УДК 629.584**
DOI: 10.34046/aumsuomt101/28

# АНАЛИЗ ЭКСПЕРЕМЕНТОВ ИССЛЕДОВАНИЯ УПРАВЛЕНИЯ СИСТЕМОЙ «СУДНО-ЗАБОРТНОЕ ОБОРУДОВАНИЕ» В ПРОДОЛЬНО-ПОПЕРЕЧНОЙ ПЛОСКОСТИ

*И.М. Данцевич, кандидат технических наук, доцент*
*А.В. Черкасов, кандидат технических наук, доцент*
*М.Н. Лютикова, кандидат технических наук, доцент*

Проведен анализ натурного эксперимента геофизического комплекса (буксируемое судно - буксируемый аппарат), с целью отработки технологии движения комплекса вдоль линии заданного профиля. Применение буксируемых геофизических систем с требуемыми параметрами качества диктуется требованиями получения качественных сонограмм исследования шельфа и безопасности проведения исследований.